

PCT/JP03/09755

22.08.03

日 本 国 特 許 庁
JAPAN PATENT OFFICE

REC'D 10 OCT 2003

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2002年10月11日

出 願 番 号
Application Number: 特願2002-298309
[ST. 10/C]: [JP2002-298309]

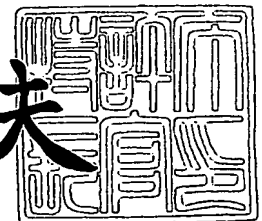
出 願 人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 9月26日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 0290539802

【提出日】 平成14年10月11日

【あて先】 特許庁長官殿

【国際特許分類】 E05B 49/00
G08B 23/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 油井 康二

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 松村 広幸

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 八重樫 章

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100091546

【弁理士】

【氏名又は名称】 佐藤 正美

【電話番号】 03-5386-1775

【手数料の表示】

【予納台帳番号】 048851

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9710846

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子鍵装置およびドアロック制御システム

【特許請求の範囲】

【請求項 1】

生体情報を取得する生体情報取得手段と、
前記生体情報が記憶されている生体情報記憶部と、
電子鍵情報が記憶されている電子鍵情報記憶部と、
前記電子鍵情報を外部に送信する機能を備える通信手段と、
前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、
前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する制御手段と、
を備えることを特徴とする電子鍵装置。

【請求項 2】

前記生体情報取得手段は、前記生体情報として指紋情報を取得するものであることを特徴とする請求項 1 に記載の電子鍵装置。

【請求項 3】

前記生体情報取得手段は、前記生体情報として虹彩情報を取得するものであることを特徴とする請求項 1 に記載の電子鍵装置。

【請求項 4】

前記電子鍵情報は、同一のものが存在しないように一元管理されて割り振られた識別情報であることを特徴とする請求項 1 に記載の電子鍵装置。

【請求項 5】

電子鍵情報を記憶する電子鍵装置と、前記電子鍵装置からの前記電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置とからなるドアロック制御システムであって、
前記電子鍵装置は、
生体情報を取得する生体情報取得手段と、
前記生体情報が記憶されている生体情報記憶部と、

電子鍵情報が記憶されている第 1 の電子鍵情報記憶部と、
前記電子鍵情報を外部に送信する機能を備える第 1 の通信手段と、
前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、
前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する第 1 の制御手段と、
を備え、
前記制御装置は、
電子鍵情報を記憶する電子鍵装置からの前記電子鍵情報の受信を行なうための第 2 の通信手段と、
電子鍵情報を記憶する第 2 の電子鍵情報記憶部と、
前記第 2 の通信手段を通じて前記電子鍵装置から受信した前記電子鍵情報と、
前記第 2 の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて前記ドアロック機構を制御する第 2 の制御手段と、
を備えることを特徴とするドアロック制御システム。

【請求項 6】

請求項 5 に記載のドアロック制御システムにおいて、
前記電子鍵装置の前記生体情報取得手段は、前記生体情報として指紋情報を取得するものであることを特徴とするドアロック制御システム。

【請求項 7】

請求項 5 に記載のドアロック制御システムにおいて、
前記電子鍵装置の前記生体情報取得手段は、前記生体情報として虹彩情報を取得するものであることを特徴とするドアロック制御システム。

【請求項 8】

請求項 5 に記載のドアロック制御システムにおいて、
前記電子鍵情報は、同一のものが存在しないように一元管理されて割り振られた識別情報であり、
前記制御装置は、前記電子鍵情報に対応して前記電子鍵装置の所有者を特定可能とする個人情報を記憶する個人情報記憶部を備えるとともに、前記電子鍵装置

から受信した前記電子鍵情報と、前記第2の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて、前記電子鍵装置の所有者の前記ドアからの入退出を管理する手段を備える

ことを特徴とするドアロック制御システム。

【請求項9】

請求項5に記載のドアロック制御システムにおいて、

前記電子鍵情報は、前記制御装置ごとに、同一のものが存在しないように一元管理されて割り振られた識別情報である

ことを特徴とするドアロック制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ドアの施錠、開錠を制御するための電子鍵情報を外部に送出する機能を有する電子鍵装置および当該電子鍵装置と通信を行なって前記電子鍵情報を用いてドアの施錠、開錠を制御するようにするドアロック制御システムに関する。

【0002】

【従来の技術】

最近、従来の物理的な鍵を鍵シリンダーに差し込んで施錠、開錠を行なうドアロック制御システムを玄関ドアなどに採用している住戸等においては、鍵シリンダー機構に精通しているものが、鍵を用いずに開錠することによる盗難等の事件が発生している。

【0003】

そこで、このような鍵シリンダー機構を用いない電子鍵によるドアロック制御システムが注目されている。例えば、この電子鍵によるドアロックシステムの一例として、親機は、予め登録されている電子鍵情報としてのIDコードと、電子鍵情報としての子機から受信したIDコードを比較照合して、その比較結果に基づいてドアロックをコントロールするものが知られている（例えば特許文献1（特開平9-4293号公報参照））。

【0004】

【特許文献1】

特開平9-4293号公報。

【0005】

【発明が解決しようとする課題】

ところで、鍵を紛失した場合には、ドアロック機構の鍵シリンダーを当該鍵以外の鍵を用いるものに交換しない限り、悪意の紛失鍵の拾得者にドアが開錠されてしまうおそれがつきまとう。電子鍵によるドアロックシステムにおいても、電子鍵情報が書き込まれている装置（以下、電子鍵装置と称する）を紛失してしまった場合には、上述した悪意の紛失鍵の拾得者に対抗する対策が必要である。

【0006】

この発明は、紛失しても、容易に悪意の紛失鍵の拾得者に対抗することができる電子鍵装置および当該電子鍵装置を用いるドアロック制御システムを提供することを目的とする。

【0007】

【課題を解決するための手段】

上記課題を解決するために、請求項1の発明による電子鍵装置は、
生体情報を取得する生体情報取得手段と、
前記生体情報が記憶されている生体情報記憶部と、
電子鍵情報が記憶されている電子鍵情報記憶部と、
前記電子鍵情報を外部に送信する機能を備える通信手段と、
前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、
前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する制御手段と、
を備えることを特徴とする。

【0008】

請求項1の発明による電子鍵装置においては、予め登録された所有者の生体情報が確認されたときにのみ、電子鍵情報を送出するように制御することができる

ので、当該電子鍵装置を紛失したとしても、電子鍵装置の電子鍵情報記憶部に登録された生体情報と一致しない悪意の拾得者の使用を阻止することができるものである。

【0009】

そして、請求項4の発明のように、電子鍵情報として、同一のものが存在しないように一元管理されて割り振られた識別情報を用いた場合には、個人の生体情報が確認されたときにのみ、電子鍵情報を送出するように制御することができるので、電子鍵情報は、個人識別情報として使用することができる。

【0010】

また、請求項5の発明によるドアロック制御システムは、
電子鍵情報を記憶する電子鍵装置と、前記電子鍵装置からの前記電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置とからなるドアロック制御システムであって、

前記電子鍵装置は、
生体情報を取得する生体情報取得手段と、
前記生体情報が記憶されている生体情報記憶部と、
電子鍵情報が記憶されている第1の電子鍵情報記憶部と、
前記電子鍵情報を外部に送信する機能を備える第1の通信手段と、
前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、

前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する第1の制御手段と、

を備え、
前記制御装置は、
電子鍵情報を記憶する電子鍵装置からの前記電子鍵情報の受信を行なうための第2の通信手段と、

電子鍵情報を記憶する第2の電子鍵情報記憶部と、
前記第2の通信手段を通じて前記電子鍵装置から受信した前記電子鍵情報と、
前記第2の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較

結果に基づいて前記ドアロック機構を制御する第2の制御手段と、
を備えることを特徴とする。

【0011】

この請求項5の発明によるドアロック制御システムにおいては、電子鍵装置からは、個人の生体情報が確認されたときにのみ、電子鍵情報が送出され、当該電子鍵情報が制御装置で、予め記憶されている電子鍵情報と比較して認証が取られることによりドアロック制御される。

【0012】

したがって、当該電子鍵装置を紛失したとしても、電子鍵装置の電子鍵情報記憶部に登録された生体情報と一致しない悪意の拾得者の使用を阻止することができるものである。

【0013】

また、請求項8の発明は、請求項5に記載のドアロック制御システムにおいて

、
前記電子鍵情報は、同一のものが存在しないように一元管理されて割り振られた識別情報であり、

前記制御装置は、前記電子鍵情報に対応して前記電子鍵装置の所有者を特定可能とする個人情報を記憶する個人情報記憶部を備えるとともに、前記電子鍵装置から受信した前記電子鍵情報と、前記第2の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて、前記電子鍵装置の所有者の前記ドアからの入退出を管理する手段を備える

ことを特徴とする。

【0014】

この請求項8の発明によるドアロック制御システムによれば、電子鍵情報として、同一のものが存在しないように一元管理されて割り振られた識別情報が用いられているので、制御装置では、ドアロック制御機構の制御を行なうとともに、電子鍵情報を個人識別情報として使用して、電子鍵装置の使用者毎のドアを通じての入退出を管理することができる。

【0015】

【発明の実施の形態】

以下、この発明によるドアロック制御システムの実施形態を、図を参照しながら説明する。

【0016】

以下に説明する例では、家の玄関ドアに、実施形態のドアロック制御システムを設ける。また、この例では、家の中には、窓や玄関ドアからの賊の侵入、火災の発生、ガス漏れを検知して、それぞれの異常事態に対応する措置を取るセキュリティ監視システムを設け、このセキュリティ監視システムとドアロック制御システムとを、通信可能に接続して連動させて動作させるようにしている。

【0017】

そして、さらに、この例では、セキュリティ監視システムは、通信ネットワークを通じて管理サーバ装置に接続して、全体として、通信システムを構成している。

【0018】

この場合に、電子鍵装置は、生体情報取得部と、制御用 IC (Integrated Circuit) と、通信手段とを備えるもので、種々の形態のものが使用可能である。この例では、この電子鍵装置の具体例としては、ICカードの他、携帯電話端末、PDA (Personal Digital Assistants) 端末などを用いることもできる。

【0019】

電子鍵装置に搭載される制御用 IC は電子鍵情報用メモリを備え、その電子鍵情報用メモリには、電子鍵情報が格納されている。この電子鍵情報としては、この例では、同一のものが存在しないように一元管理された識別情報が記憶される。この例では、この識別情報としては、ICチップ製造番号が用いられる。

【0020】

例えば、図1に示すように、1社あるいは複数社のICチップの製造会社1001において、製造した制御用ICチップ1002に対して、一元管理された重複のないICチップ製造番号を付与するようにする。ICチップの製造会社1001が複数社の場合には、例えば、それぞれのICチップ製造会社1001に、

予め、制御用 IC チップ 1002 に付与する製造番号を割り当てておくようにすることにより、一元管理される。したがって、製造された制御用 IC チップ 1002 のメモリには、互いに異なる IC チップ製造番号が識別情報として記憶される。

【0021】

この制御用 IC チップ 1002 は、IC カード製造工場（あるいは製造会社）1003、携帯電話端末製造工場（あるいは製造会社）1004、PDA 端末製造工場（あるいは製造会社）1005 などに供給されて、それらの制御用 IC チップと通信手段とが搭載された IC カード、携帯電話端末、PDA 端末などが製造される。

【0022】

図 2 は、この実施形態で用いられる IC チップ製造番号の一例を説明するための図である。

【0023】

この例の IC チップ製造番号は、3桁のメーカー番号と、3桁のカテゴリコードと、4桁のシリアル番号とからなる、合計 10桁の番号（記号を含む）で構成される。

【0024】

なお、識別情報は、IC チップ製造番号の限定されるものではなく、同一のものが存在しないように一元管理された情報であれば、どのようなものも使用可能である。また、識別情報は、IC チップ製造番号と共に、別個に IC のメモリに記憶するようにしてもよい。

【0025】

電子鍵装置の通信手段としては、この例では、電磁誘導や電波を用いた非接触による通信手段が用いられる。この実施形態においては、この通信手段は、例えば数ミリメートル～数十センチメートルの範囲で通信ができるものであればよく、小パワーのもので十分である。

【0026】

次に、この実施形態のドアロック制御システムにおいては、玄関ドアには、電

子鍵装置によりドアの施錠、開錠を行なえるようにするためのドアロック装置が取り付けられる。この例では、電子鍵装置とドアロック装置との間では、電子鍵情報の通信を行ない、ドアロック装置は、その通信に基づいてドアの施錠、開錠を制御するようにする。

【0027】

以下に説明する例では、電子鍵装置とドアロック装置との間の通信は、電磁誘導を用いた非接触による通信とされており、後述するように、ドアロック装置の一部を構成する電子鍵装置のリード／ライト部を介して、通信が行われる。

【0028】

この実施形態では、ドアの施錠、開錠を制御するための電子鍵情報としては、前述したICチップ製造番号からなる識別情報が用いられる。この実施形態では、当該家における電子鍵情報として、前述のようにして一元管理された識別情報が内蔵メモリに書き込まれた電子鍵装置の前記識別情報を電子鍵情報として管理サーバ装置に登録することにより、家族構成員のそれぞれが、自分用の電子鍵装置を所有して使用するようになる。

【0029】

この実施の形態では、管理サーバ装置は、登録された家族構成員のそれぞれについての電子鍵情報をドアロック装置の電子鍵情報の記憶部に転送して、電子鍵情報をドアロック装置に登録させるようにする。ドアロック装置は、登録された電子鍵情報と、通信装置としての電子鍵装置から受信した電子鍵情報とを比較し認証して、その結果に応じてドアの施錠、開錠を制御する。

【0030】

後述するように、この実施形態では、家族構成員のそれぞれは、自分用の電子鍵情報として、本鍵情報と、バックアップ鍵情報とを管理サーバ装置に登録することができる。電子鍵情報は、前述したように、電子鍵装置ごとに異なるので、本鍵情報とバックアップ鍵情報との登録は、本鍵装置と、バックアップ鍵装置との登録に等しい。

【0031】

以下に説明する例においては、各人に与えられる本鍵装置としては、ドアロッ

ク制御システムの提供会社が提供する I C カードとされる。そして、この本鍵装置である I C カードの識別情報が、ドアロック制御システムが当該家に取り付けられる前に、予め管理サーバ装置に、当該 I C カードの所有者の電子鍵情報として登録される。

【0032】

この場合に、この実施形態では、家族構成員の数分だけ、I C カードが前記提供会社から提供され、それらの複数の I C カードの全ての識別情報が、設置されるドアロック制御システム用の電子鍵情報として管理サーバ装置に登録される。

【0033】

さらに、この実施形態では、管理サーバ装置には、ドアロック制御システムが設置される家の家族構成員のそれぞれについての個人情報が収集され、その個人情報に対応して、それぞれの家族構成員が持つ I C カードの識別情報が登録される。したがって、ドアロック制御システムは、電子鍵情報を検索することにより、それが誰の電子鍵情報であるかを判別することができる。つまり、この例の通信システムにおいては、電子鍵情報を、家族構成員の個人識別情報として用いることが可能である。

【0034】

そして、管理サーバ装置に登録された各家族構成員の本鍵情報は、ドアロック制御システムが、当該家に設置された後、システムの設置事業者や、ユーザが管理サーバ装置に対して初期登録要求をすることにより、ドアロック装置の記憶部に登録され、電子鍵情報の認証用として使用されることになる。

【0035】

また、この実施形態では、本鍵装置を紛失してしまった場合を考慮して、バックアップ鍵情報を登録しておくことができる。後述するように、この実施形態では、バックアップ鍵情報は、家族構成員の各人が、バックアップ鍵装置として使用したい電子鍵装置の識別情報（この例では、I C 製造番号）を管理サーバ装置に登録することにより、登録可能である。

【0036】

なお、本鍵情報とバックアップ鍵情報との電子鍵情報の認証についての取り扱い

い方法としては、本鍵情報とバックアップ鍵情報とを同等に扱う方法と、認証用としては本鍵情報のみを原則とし、本鍵情報が抹消されたときに、バックアップ鍵情報が登録されていれば、以後は、バックアップ鍵情報を本鍵情報として取り扱うようにする方法とがある。いずれの方法を用いることができるが、できるだけ、認証用としては、少ない方がセキュリティ上は好ましいと考えられるので、この実施形態では、後者の場合を採用するものとしている。

【0037】

前述したように、この実施形態においては、電子鍵情報として用いる識別情報は、個人識別情報としても用いることができることを利用して、各家族構成員個々の玄関ドアからの入退出を管理することができるようにする。

【0038】

このように電子鍵情報を個人識別情報としても用いることにより、当該家に住む家族構成員それぞれの玄関ドアからの入退出の管理情報を、セキュリティシステムに反映させることができ、より高機能のセキュリティシステムを構築することができる。

【0039】

[実施形態のドアロックシステムを含むセキュリティシステムの概要]

図3は、ドアロック制御システムおよびセキュリティシステムを含む、この実施形態の通信システムの概要を説明するための図である。

【0040】

家の玄関ドア1には、電子鍵装置と通信を行なうドアロック装置2が取り付けられている。室内には、セキュリティシステムを構成する監視制御装置3が設けられ、ドアロック装置2と接続されている。ドアロック装置2と監視制御装置3とは、この例では接続線により接続されるが、無線により接続するようにしてもよい。

【0041】

監視制御装置3は、ドアロック装置2からの電子鍵情報を受け取って、前述した電子鍵情報の認証を行なう装置、つまり認証装置となることもできる。しかし、この例では、電子鍵情報の認証は、ドアロック装置2自身において行なうよう

にされている。

【0042】

そして、この例では、室内には、火災発生を検知する火災センサ4と、ガス漏れを検知するガスセンサ5と、窓の戸締りを検知する窓センサ6a, 6bと、テレビ7が設けられ、それぞれ監視制御装置3に接続されている。監視制御装置3とそれらとの接続も、接続線により接続されているが、無線により接続してもよい。

【0043】

また、図3では省略したが、火災センサ4で火災発生を検知したときに、その発生現場近傍を撮影できるような位置や、窓センサ6a, 6bで賊の侵入を検知したときに、その賊を撮影できるような位置には、監視カメラを設けるようにすることができる。その場合には、それら監視カメラは監視制御装置3に接続され、監視カメラの撮影画像が監視制御装置3に供給されるようにされる。

【0044】

監視制御装置3は、また、電話回線8を通じ、通信ネットワーク9を通じてセキュリティシステムの管理会社が運営する管理サーバ装置10に接続される。この管理サーバ装置10も、ドアロック装置2からの電子鍵情報を、監視制御装置3を介して受け取ることにより、電子鍵情報の認証を行なう装置となることもできる。

【0045】

通信ネットワーク9は、携帯電話網をも含み、後述するように、監視制御装置3は、異常状態の発生時に、予め登録された携帯電話端末11a, 11bに、当該異常状態の発生を知らせることが可能とされている。さらに、通信ネットワーク9は、インターネットを含み、パーソナルコンピュータ12は、管理サーバ装置10に対して当該インターネットを通じてアクセスすることが可能とされている。また、携帯電話端末11a, 11bからも、管理サーバ装置10にアクセスすることが可能とされている。

【0046】

なお、この実施形態においては、特許請求の範囲における制御装置は、ドアロ

ック装置 2 の後述するドアロック制御装置と監視制御装置とで構成されるものである。

【0047】

次に、ドアロック装置 2 の具体的構成例およびその動作、また、監視制御装置 3 の具体的構成例およびその動作について、詳細に説明する。なお、以下に説明する例では、前述したように、電子鍵情報の認証は、ドアロック装置自身が行なうものとする。

【0048】

[電子鍵装置の構成例]

前述したように、この実施形態においては、電子鍵装置としては、ICカードの他、携帯電話端末やPDA端末なども用いることができる。しかし、電子鍵装置は、生体情報の取得部と、制御用ICチップと、通信手段とを備える点では共通している。電子鍵装置がICカードである場合の構成例を次に示す。

【0049】

<電子鍵装置の第1の例>

この第1の例の電子鍵装置は、生体情報として、指紋を用いるICカードの場合の例である。図4(A)は、この例のICカード40Fの表面を示し、この表面には、所有者の氏名と、ID番号が表示されていると共に、指紋読取部41の指紋読取窓41Wが形成されている。

【0050】

また、図4(B)は、ICカード40Fの内部構成例を示しており、ICカード40F内には、指紋読取部41と、後述するドアロック装置2の電子鍵リード／ライト部と通信を行なうための電磁誘導アンテナ42と、制御用IC43と、情報送受信回路部44が内蔵されている。

【0051】

指紋読取部41は、指紋読取窓41Wに置かれた指の指紋を読み取り、その読み取った指紋の情報を制御用IC43に送る。制御用IC43は、予め登録されて記憶しているICカード40Fの所有者の指紋情報と、読み取った指紋情報とを比較し、一致しているかどうか判別する。

【0052】

そして、一致していると判別すると、予め制御用 IC 43 内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部 44 および電磁誘導アンテナ 42 を通じて、外部に送出する。記憶している指紋情報と、読み取った指紋情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

【0053】

図 5 は、第 1 の例の場合の IC カード 40 F の内部ブロック構成を示すものである。CPU (Central Processing Unit) 401 に対してシステムバス 402 を介してプログラムやデータが記録されている ROM (Read Only Memory) 403 と、ワークエリア用 RAM (Random Access Memory) 404 と、電子鍵情報となる識別情報が記憶されている識別情報メモリ 405 と、通信履歴メモリ 406 と、送受信インターフェース 407 と、指紋登録メモリ 408 と、指紋読取部インターフェース 409 と、指紋照合部 410 とが接続されている。

【0054】

識別情報メモリ 405 には、前述した IC 製造番号からなる識別情報が記憶されている。なお、この IC カード 40 の所有者の氏名、住所の他、所有者のその他の必要な個人情報を記憶することもできる。この個人情報は、父親、母親、子供などの区別が可能なように構成される。

【0055】

通信履歴メモリ 406 には、各所有者が行ったドアロック装置 2 の後述する電子鍵リード／ライト部との通信の時刻や履歴（内側と外側のどちらの電子鍵リード／ライト部と通信したか情報を含む）や、各所有者の外出、帰宅の履歴などを書き込むことが可能とされている。なお、これらの履歴情報は、後述するように、ドアロック装置 2 のメモリや監視制御装置 3 のメモリにおける家族構成員の各人に対応するエリアにも記憶されるものである。

【0056】

送受信インターフェース 407 には、電磁誘導アンテナ 41 に接続されている

情報送受信回路部 44 が接続されている。

【0057】

指紋登録メモリ 408 には、当該 IC カード 40F の所有者の指紋の情報が予め登録されて記憶されている。指紋読取部インターフェース 409 は、指紋読取部 41 で読み取った指紋の情報を取り込むためのものである。指紋照合部 410 は、指紋読取部インターフェース 409 を通じて取得した指紋の情報と、指紋登録メモリ 408 から読み出した前記所有者の指紋の情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス 402 に送出する。指紋照合部 410 は、ハードウェアの構成ではなく、CPU 401 によるソフトウェアによる構成とすることもできる。

【0058】

CPU 401 は、前述したように、指紋照合部 410 での判定結果に基づき、指紋一致、つまり、指紋照合が OK であったときには、識別情報メモリ 405 から読み出した識別情報からなる電子鍵情報を、送受信インターフェース 407、情報送受信回路 408 および電磁誘導アンテナ 41 を通じて送出し、指紋照合部 410 での判定結果が指紋不一致、つまり、指紋照合が NG であったときには、電子鍵情報の送出を禁止する。

【0059】

また、CPU 401 は、電磁誘導アンテナ 42 にて受信した情報を、情報送受信回路部 408 および送受信インターフェース 407 を通じて取り込み、通信履歴メモリ 406 に書き込んだりする処理も行なう。

【0060】

図 6 は、このときの CPU 401 での処理動作を説明するためのフローチャートである。

【0061】

CPU 401 は、指紋読取部インターフェース 409 を通じた指紋読取部 41 からの指紋情報の受信を待ち（ステップ S1）、指紋情報を受信したと判別したときには、指紋登録メモリ 408 に登録されている所有者の指紋情報を読み出し、指紋照合部 410 において指紋照合を行なわせる（ステップ S2）。

【0062】

そして、CPU401は、指紋照合部410からの指紋照合の判定結果が指紋一致であるか否か判別し（ステップS3）、指紋不一致で照合がNGであったときには、処理をそのまま終了して、電子鍵情報の送出は行なわない。

【0063】

また、CPU401は、指紋一致で照合がOKであったときには、識別情報メモリ405から識別情報を読み出して、電子鍵情報として、情報送受信回路部44および電磁誘導アンテナ42を通じて送出する（ステップS4）。

【0064】

そして、CPU401は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップS5）、電磁誘導アンテナ42、情報送受信回路部44および送受信インターフェース407を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ406に書き込み（ステップS6）、その後、この処理ルーチンを終了する。

【0065】

ステップS5で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、CPU401は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップS7）、所定時間経過していないと判別したときには、ステップS4に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップS7で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

【0066】

以上のように、この例の電子鍵装置としてのICカード40Fによれば、予め登録してある所有者の指紋と、使用者の指紋とを照合して、照合がOKである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

【0067】

<電子鍵装置の第2の例>

この第2の例の電子鍵装置は、生体情報として、虹彩を用いるICカードの場合の例である。図7(A)は、この例のICカード40Iの表面を示し、この表面には、所有者の氏名と、ID番号が表示されていると共に、使用者の虹彩を読み取るための手段として、この例では、CCD (Charge Coupled Device) カメラ45が設けられている。

【0068】

また、図7(B)は、ICカード40Iの内部構成例を示しており、ICカード40I内には、第1の例のICカード40Fと同様に、電磁誘導アンテナ42と、制御用IC43と、情報送受信回路部44とが内蔵されていると共に、CCDカメラ45からの撮像信号を処理して制御用IC43に供給するための撮像信号処理回路部46が内蔵されている。

【0069】

使用者は、CCDカメラ45により自分の目(虹彩)を撮影させる。CCDカメラ45は、撮影した使用者の虹彩情報を撮像信号処理回路部46を通じて取り込み、その取り込んだ虹彩の情報を制御用IC43に送る。制御用IC43は、予め登録されて記憶されているICカード40Iの所有者の虹彩情報と、取り込んだ虹彩情報とを比較し、一致しているかどうか判別する。

【0070】

そして、一致していると判別すると、予め制御用IC43内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部44および電磁誘導アンテナ42を通じて、外部に送出する。記憶している虹彩情報と、取り込んだ虹彩情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

【0071】

図8は、第2の例の場合のICカード40Iの内部ブロック構成を示すものである。この第2の例においては、図5の第1の例の指紋登録メモリ408と、指紋読取部インターフェース409と、指紋照合部410とに代わって、虹彩情報登録メモリ411と、撮像信号インターフェース412と、虹彩照合部413とが設けられる。撮像信号インターフェース412は、CCDカメラ45に接続さ

れている。その他の構成は、第1の例の図5と同様である。

【0072】

虹彩情報登録メモリ411には、当該ICカード401の所有者の虹彩の情報が予め登録されて記憶されている。撮像信号インターフェース412は、撮像信号処理回路部46からの虹彩情報を取り込むためのものである。虹彩照合部413は、撮像信号インターフェース412を通じて取り込んだ虹彩情報と、虹彩情報登録メモリ411から読み出した前記所有者の虹彩情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス402に送出する。虹彩照合部413は、ハードウェアの構成ではなく、CPU401によるソフトウェアによる構成とすることもできる。

【0073】

CPU401は、虹彩照合部413での判定結果に基づき、虹彩一致、つまり、虹彩照合がOKであったときには、識別情報メモリ405から読み出した識別情報からなる電子鍵情報を、送受信インターフェース407、情報送受信回路408および電磁誘導アンテナ41を通じて送出し、虹彩照合部413での判定結果が虹彩不一致、つまり、虹彩照合がNGであったときには、電子鍵情報の送出を禁止する。

【0074】

図9は、このときのCPU401での処理動作を説明するためのフローチャートである。

【0075】

CPU401は、撮像信号インターフェース412を通じた撮像信号処理回路部46からの虹彩情報の受信を待ち（ステップS11）、虹彩情報を受信したと判別したときには、虹彩情報登録メモリ411に登録されている所有者の虹彩情報を読み出し、虹彩照合部413において虹彩照合を行なわせる（ステップS12）。

【0076】

そして、CPU401は、虹彩照合部413からの虹彩照合の判定結果が虹彩一致であるか否かを判別し（ステップS13）、虹彩不一致で照合がNGであった

ときには、処理をそのまま終了して、電子鍵情報の送出は行なわない。

【0077】

また、CPU401は、虹彩一致で照合がOKであったときには、識別情報メモリ405から識別情報を読み出して、電子鍵情報として、情報送受信回路部44および電磁誘導アンテナ42を通じて送出する（ステップS14）。

【0078】

そして、CPU401は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップS15）、電磁誘導アンテナ42、情報送受信回路部44および送受信インターフェース407を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ406に書き込み（ステップS16）、その後、この処理ルーチンを終了する。

【0079】

ステップS15で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、CPU401は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップS17）、所定時間経過していないと判別したときには、ステップS14に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップS7で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

【0080】

以上のように、この第2の例の電子鍵装置としてのICカード401によれば、予め登録してある所有者の虹彩と、使用者の虹彩とを照合して、照合がOKである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

【0081】

〔生体情報の他の例〕

以上の例では、生体情報としては、指紋と、虹彩の場合について説明したが、生体情報としては、これに限られるものではない。例えば手の甲の静脈パターンを生体情報として用いることもできる。この場合には、虹彩情報に代えて、所有

者の手の甲の静脈パターンを登録して記憶しておくとともに、CCDカメラ45により、手の甲の静脈パターンを撮影して取り込むことにより、第2の例のICカード40Iの構成をそのまま用いることができる。

【0082】

なお、以上の例に限らず、個人識別が可能な生体情報であって、所定の手段により取得可能なものであれば、どのような生体情報も、利用することができることは勿論である。

【0083】

[ドアロック装置の構成]

図10(A)および図10(B)は、ドアロック装置2の構成例を説明するための図である。図10(A)は、家の外側から玄関ドア1のドアロック装置2の取り付け部分近傍を見た図である。また、図10(B)は、玄関ドア1のドアロック装置2の取り付け部分近傍を、玄関ドア1の端面側から見た図である。

【0084】

この例のドアロック装置2においては、玄関ドア1の外側（戸外側）には、電子鍵装置の例としてのICカード40Fや40Iと通信を行なうための外側電子鍵リーダ／ライタ部21exと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を視覚的に知らせるための表示素子の例としての外側LED（Light Emitting Diode；発光ダイオード）22exと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を音声により知らせるための外側スピーカ23exと、外側ドアノブ24exとが設けられている。

【0085】

また、玄関ドア1の内側（屋内側）にも、電子鍵装置の例としてのICカード40Fや40Iと通信を行なうための内側電子鍵リーダ／ライタ部21inと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を視覚的に知らせるための表示素子の例としての内側LED22inと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を音声により知らせるための内側スピーカ23inと、内側ドアノブ24inとが設けられている。

【0086】

玄関ドア 1 には、さらに、玄関ドア係止片 25 と、ロック片 26 と、ドア開閉センサ 27 が設けられている。さらに、玄関ドア 1 の内側には、ドアロック装置 2 の動作を制御するためのドアロック制御装置 100 が設けられており、電子鍵リーダ／ライタ部 21 ex および 21 in、LED 22 ex および 22 in、スピーカ 23 ex および 23 in、ドア開閉センサ 27 および図示を省略したドアロック機構駆動部が、このドアロック制御装置 100 に接続されている。

【0087】

玄関ドア係止片 25 は、ドアノブ 24 ex あるいはドアノブ 24 in の操作に応じて、玄関ドアの端面 1 a に垂直な方向に摺動移動する部材である。これは、後述するオートロックモードでない場合において、玄関ドア 1 が施錠されていないときにも、玄関ドア 1 の端面 1 a と対向する壁の端面側に設けられる凹部に勘合して、玄関ドア 1 を、係止するためのものである。

【0088】

ロック片 26 は、ドアロック機構の一部を構成する部材であり、図 10 では図示を省略したドアロック機構駆動部によりドアロック機構が駆動されることにより、玄関ドアの端面 1 a に垂直な方向に摺動移動して、玄関ドア 1 を施錠するときには、図 10 のように、玄関ドア 1 の端面 1 a から突出する状態に固定され、玄関ドア 1 を開錠するときには、玄関ドア 1 の端面 1 a から突出しない状態に固定される。

【0089】

なお、図示は省略したが、玄関ドア 1 の端面 1 a と対向する壁の端面には、このロック片 26 が突出した状態のときに嵌合される凹部が形成されており、ロック片 26 が当該凹部に嵌合される状態が玄関ドアの施錠状態となる。そして、ロック片 26 が玄関ドア 1 側に引っ込んで、当該凹部に嵌合していないときには、施錠状態が解除されて、開錠状態になる。

【0090】

玄関ドア開閉センサ 27 は、例えば光学式センサが用いられ、玄関ドア 1 が開けられたときは外部光を検知することにより、それを検知し、玄関ドア 1 が閉じられたときには、玄関ドア 1 の端面 1 a が、壁の端面と衝合することにより外部

光が遮断されることを検知することにより、それを検知して、玄関ドア 1 の開閉を検知する。

【0091】

[ドアロック制御装置 100 の説明]

次に、ドアロック制御装置 100 を中心にしたドアロック装置 2 の電氣的な構成例を図 11 に示す。なお、以下の説明においては、電子鍵装置としては、指紋照合認証を行なう第 1 の例の IC カード 40F を用いるものとする。

【0092】

すなわち、ドアロック制御装置 100 は、マイクロコンピュータの構成を備えており、CPU (Central Processing Unit) 101 に対してシステムバス 102 を介してプログラムやデータが記録されている ROM (Read Only Memory) 103 と、ワークエリア用 RAM (Random Access Memory) 104 と、家族構成員の個々についての電子鍵情報となる識別情報 (この例では、IC 製造番号) が記憶されている家族情報メモリ 120 と、監視制御装置 3 と通信を行なうための通信インターフェース 121 とが接続されている。

【0093】

家族情報メモリ 120 には、後述するように、管理サーバ装置 10 に登録された本鍵情報やバックアップ鍵情報が、家族構成員のそれぞれについて、電子鍵情報として登録されて格納されている。また、各家族構成員を識別するための情報、例えば、氏名、年齢、性別、続柄、その他の個人情報も、併せて家族情報メモリ 120 に格納するようにしてもよい。この家族情報メモリ 120 への電子鍵情報の登録に関しては、後述する。

【0094】

また、システムバス 102 には、インターフェース 105 および 106 を介して内側電子鍵リード／ライト部 21in および外側電子鍵リード／ライト部 21ex が接続され、また、内側 LED 駆動部 107 を介して内側 LED 22in が接続され、外側 LED 駆動部 108 を介して外側 LED 22ex が接続され、さらに、音声出力インターフェース 109 を介して内側スピーカ 23in が接続さ

れ、音声インターフェース 110 を介して外側スピーカ 23ex が接続される。

【0095】

さらに、システムバス 102 には、インターフェース 111 を介してドア開閉センサ 27 が接続されると共に、ドアロック機構駆動部 112 を介して、ロック片 26 を摺動駆動させるドアロック機構 28 が接続される。

【0096】

電子鍵リード／ライト部 21ex または 21in は、IC カード 40F（または 40I）と通信を行なう通信部を構成する。電子鍵リード／ライト部 21ex または 21in は、この例では、電磁誘導アンテナおよび情報送受信部を含む。

【0097】

この例のドアロック制御装置 100 は、ドアロック制御モードとして、オートロックモードと、逐次ロックモードとの 2通りの制御モードを備えている。

【0098】

オートロックモードは、ドアロック制御装置 100 が、電子鍵リード／ライト部 21ex, 21in を介して IC カード 40F と通信することに基づき玄関ドア 1 を開錠した後、所定時間後に自動的に玄関ドアを施錠状態にするモードである。オートロックモードにおいては、常に、内側と外側の電子鍵リード／ライト部 21ex, 21in の両方を用いるものとなる。

【0099】

また、逐次ロックモードは、少なくとも玄関ドア 1 の外側の電子鍵リード／ライト部 21ex を通じて IC カード 40F と通信することに基づき玄関ドアの施錠、開錠の状態を、そのときの状態とは逆の状態にするモードである。この逐次ロックモードにおいても、内側と外側の電子鍵リード／ライト部 21ex, 21in の両方を用いることができるが、内側は、別途のマニュアルの施錠手段により施錠するようにした場合には、外側の電子鍵リード／ライト部 21ex を通じた IC カード 40F との通信のみにより、玄関ドアの施錠、開錠動作を行なわせるようにすることができる。この逐次ロックモードは、従来からの一般的な鍵による施錠、開錠の方法に合わせたモードである。

【0100】

ドアロック装置 2 のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、この例では、例えば、ドアロック装置 2 を取り付ける際に、後述するように、作業者により監視制御装置 3 を通じて行なわれる。

【0101】

ドアロック装置 2 がいずれのドアロック制御モードに設定されているかの情報は、ドアロック制御装置 100 内の図示を省略した不揮発性メモリに格納されており、ドアロック制御装置 100 は、当該不揮発性メモリの記憶情報を参照することにより、自装置のドアロック制御モードが、オートロックモードか、逐次ロックモードかを認識するものである。監視制御装置 3 を通じたドアロック制御モードの設定動作に関しては、後述する。

【0102】

なお、ドアロック装置 2 のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、監視制御装置 3 を通じて行なうのではなく、ドアロック装置 2 に直接的に行なうようにすることもできる。例えば、予め、ドアロック装置 2 の出荷時に、いずれのドアロック制御モードにするかの設定をドアロック装置 2 に行なっておくようにしても良い。また、ドアロック装置 2 に、ドアロック装置 2 の設置作業者が操作可能な入力操作手段、例えばディップスイッチ等を設けておき、当該入力操作手段を通じて、ドアロック制御モードの設定を行なうようにしてもよい。

【0103】

[監視制御装置 3 の外観の説明]

図 12 は、室内に設けられるセキュリティシステム用の監視制御装置 3 の構成を説明するための外観図であり、この監視制御装置 3 は、例えば赤外線や電波を用いたリモートコマンド 50 によりリモコン制御可能の構成とされている。

【0104】

監視制御装置 3 の筐体 30 には、ビデオカメラ 31 が組み込まれている。このビデオカメラ 31 は、この例では、実線位置の横置き状態と、点線位置の縦置き状態とのいずれの状態をも取れる機構により、筐体 30 に対して取り付けられて

いる。このビデオカメラ31は、セキュリティモードがオンとされたときに、監視制御装置3からの指示により撮影を開始するようにされている。

【0105】

また、ビデオカメラ31による撮影方向は、ビデオカメラが首振り方向に調整可能な構造とされているので、その調整により変えられるようにされている。したがって、使用者は、セキュリティモードオンに先立ち、ビデオカメラ31による撮影方向の調整を行なっておくことができる。

【0106】

そして、筐体30には、ビデオカメラ31による撮影対象部を明るく照明するための撮影用ランプ32が設けられている。また、筐体30には、例えば遠赤外線を検知することにより人を検知する人感センサ33が設けられている。監視制御装置3は、後述するように、セキュリティモードオンのときに人感センサ33で人を検知したときには、賊の侵入であるとして検知し、撮影用ランプ32をオンにすると共に、所定の通報先に撮影画像を送るようにする。

【0107】

筐体30には、また、マイクロホン34とスピーカ35とが設けられている。マイクロホン34は、賊の声や賊侵入時の室内の臨場音を收音するためのものである。スピーカ35は、侵入してきた賊を威嚇する音声を放音するためなどに用いられる。

【0108】

筐体30には、また、電子鍵リード／ライト部36が設けられる。この電子鍵リード／ライト部36は、この例では、伝言の記録、再生の際に用いられる。すなわち、この例においては、監視制御装置3は、伝言装置の役割もできるように構成されており、電子鍵リード／ライト部36により、電子鍵装置としてのICカード40Fを読み取らせた後、後述するようにリモートコマンド50の伝言記録ボタンを押すと、設定した相手（家族の誰か）に伝言が残すことができ、また、リモートコマンド50の伝言再生ボタンを押すと、自分宛ての伝言を再生することができるようになっている。

【0109】

この伝言が記録されているかどうかなどを知らせるため等の用途として、筐体 30 には、複数の LED 37 が設けられている。また、筐体 30 には、さらに、リモートコマンド 50 からのリモコン信号の受信部 38 が設けられる。

【0110】

また、図 12 では図示を省略したが、監視制御装置 3 の背面パネルには、テレビ受像機 7 のビデオ入力端子に接続される映像出力端子が設けられている。そして、監視制御装置 3 には、テレビ受像機 7 の電源のオン・オフなどを制御するためのリモコン送信部 39 が設けられている。

【0111】

さらに、監視制御装置 3 は、火災センサ 4、ガスセンサ 5、窓センサ 6a、6b、さらには、監視カメラを接続するためのセンサハブを備えている。また、図 3 で説明したように、監視制御装置 3 は、電話回線を通じて、セキュリティシステムの管理会社が運営する管理サーバ装置 10 にアクセスできるように構成されている。

【0112】

[監視制御装置 3 の構成例]

監視制御装置 3 の内部構成および監視制御装置 3 と周辺機器との接続状態の構成例を図 13 に示す。

【0113】

監視制御装置 3 は、マイクロコンピュータの構成を備えており、CPU 201 に対して、システムバス 202 を介して、プログラムやデータが記録されている ROM 203 と、ワークエリア用 RAM 204 と、ドアロック制御装置 100 の家族情報メモリ 120 と同様に、電子鍵装置としての IC カード 40F または 40I を所有する家族全員の電子鍵情報となる識別情報が記憶されている家族情報メモリ 205 と、ドアロック制御装置 100 と通信を行なうためのドアロック装置通信インターフェース 206 と、センサハブ 207 と、ビデオカメラ 31 の撮影画像およびマイクロホン 34 で収音した音声を記憶するための画像・音声メモリ 208 と、電話回線を通じて管理サーバ装置 10 等と通信を行なうための通信インターフェース 209 とが接続されている。

【0114】

また、システムバス202には、カメラインターフェース210を介してビデオカメラ31が、インターフェース211を介して撮影用ランプ32の照明機構320が、インターフェース212を介して人感センサ33が、インターフェース214を介して電子鍵リード／ライト部36が、インターフェース215を介してリモコン受信部38が、インターフェース216を介してリモコン送信部39が、音声入力インターフェース218を介してマイクロホン34が、インターフェース219を介してLED37が、音声出力インターフェース220を介してスピーカ35が、それぞれ接続されている。さらに、システムバス202は、ビデオ信号出力端子からなるテレビインターフェース217を介してテレビ受像機7に接続されている。

【0115】

家族情報メモリ205は、例えばEEPROM (Electrically Erasable Programmable ROM) で構成される。

【0116】

家族情報メモリ205には、ドアロック制御装置100の家族情報メモリ120と同様に、家族構成員のそれぞれについての識別情報と、個人情報とが格納されている。この明細書では、識別情報と個人情報とからなる情報を、個人プロフィール情報と呼ぶことにする。

【0117】

後述するように、この例では、家族構成員すべての個人プロフィール情報は、ドアロック装置2および監視制御装置3が設置されたときに、設置管理者が管理サーバ装置10に初期登録依頼をすることにより、管理サーバ装置10から送られてきて、監視制御装置3に自動的に登録される。そして、監視制御装置3は、少なくとも個人プロフィール情報のうちの個人識別情報を電子鍵情報として、ドアロック制御装置100に転送する。ドアロック制御装置100は、その電子鍵情報を家族情報メモリ120に登録する。

【0118】

図14に、一人分の個人プロフィール情報の例を示す。図14に示すように、

個人プロフィール情報は、個人識別情報と個人情報とが対応付けられて記憶された情報である。この実施形態では、個人識別情報は、前述したように、電子鍵装置の各メモリに格納されている識別情報が用いられる。個人識別情報は個人情報と対応させることで、具体的に誰の識別情報であるかが判明する。この識別情報は、電子鍵情報の役割を有することは前述した通りであり、図14に示すように、電子鍵情報としては、本鍵情報とバックアップ鍵情報とが登録可能である。バックアップ鍵情報は、複数個、登録可能としてもよい。

【0119】

図14の例においては、個人情報としては、パスワード情報、氏名、住所、生年月日、年齢、続柄、登録日、銀行口座番号、電話番号、IPアドレス、趣味／嗜好情報、家の玄関8からの入退出履歴情報、電子鍵登録・紛失履歴情報などが家族情報メモリ205に記憶される。

【0120】

この例の入退出履歴情報には、外出時刻、帰宅時刻が記憶されるほか、外出中であるか、在宅であるかの在／不在フラグが含まれる。この入退出履歴情報は、監視制御装置3が玄関ドア7を通じての家族の入退出を管理するために用いられる。また、電子鍵登録・紛失履歴情報は、後述するように、管理サーバ装置10からの電子鍵情報のバックアップ登録要求や抹消要求が到来して、バックアップ登録や抹消処理をしたときに、その日付、時刻とともに、バックアップ鍵情報や抹消した電子鍵情報を、バックアップ登録および抹消の区別をして記録しておくものである。

【0121】

さらに、この例では、この家族情報メモリ205には、セキュリティモード用の情報も格納されている。すなわち、この例では、監視制御装置3では、家族構成員の在宅状況に応じて、セキュリティレベルを変更することが可能なように構成されている。図15は、セキュリティレベルと家族構成員の在宅状況との関係を示すテーブルである。また、図16は、セキュリティレベルとセキュリティ内容との対応を示すテーブルである。

【0122】

図16に示すように、この例においては、セキュリティレベルは、セキュリティレベルが高い方から順に、レベルA、レベルB、レベルC、レベルDまでであり、レベルAにおいては、窓および玄関ドアの監視、火災やガス漏れの監視、ビデオカメラ31による監視の全てを行ない、レベルBでは、ビデオカメラ31による監視は行なわずに、窓および玄関ドアの監視および火災やガス漏れの監視を行ない、レベルCでは、火災やガス漏れの監視のみを行ない、レベルDでは、監視を行なわない、という内容である。

【0123】

そして、図15に示すように、家族構成員の在宅状況のそれぞれに対して各セキュリティレベルが割り付けられる。すなわち、この例では、父親が在宅の状況では、監視を行なわないレベルDとされる。また、父親が不在であるが母親が在宅の状況では、火災やガス漏れの監視のみを行なうレベルCとされる。また、子供のみが在宅の状況では、窓および玄関ドアの監視および火災やガス漏れの監視を行なうレベルBとされる。そして、全員が不在である状況では、全ての監視を行なうレベルAとされる。

【0124】

監視制御装置3では、セキュリティモードをオンにするとき、また、セキュリティレベルを変更するとき、これら図15、図16のテーブルを参照し、在宅状況に応じてセキュリティレベルを決定するようにする。

【0125】

図15のセキュリティレベルと、家族構成員の在宅状況との関係は、予め設定しておくこともできるし、使用者が、例えばリモートコマンド50を用いて監視制御装置3に入力設定することにより、設定を変更することできるように構成されている。

【0126】

なお、これら図15、図16のテーブル情報は、家族情報メモリ205ではなく、別のメモリに格納するようにしても良いことは言うまでもない。

【0127】

ドアロック装置通信インターフェース206は、ドアロック制御装置100に

接続されている。センサハブ207には、火災センサ4、ガスセンサ5、窓センサ6a、6bおよび1個あるいは複数個の監視カメラ13が接続される。

【0128】

画像・音声メモリ208は、セキュリティモードがオンであるときに、ビデオカメラ31で撮影した画像情報と、マイクロホン34で収音した音声情報とをバッファリングする監視情報領域と、伝言として記録されている画像情報および音声情報を記憶する伝言情報領域とを備えている。また、監視情報領域には、監視カメラ13用の画像記憶領域も設けられている。

【0129】

監視情報領域は、この例では、所定時間、例えば30秒分の画像情報および音声情報を、いわゆるリングバッファ形式で記憶する。なお、監視情報領域と伝言情報領域とは、別々のメモリの構成とすることも勿論できる。

【0130】

通信インターフェース209は、この例では、ルータ61に接続されている。ルータ61は、ADSLモデム62、スプリッタ63を通じて電話回線65に接続されている。スプリッタ63には、電話端末64が接続される。

【0131】

[リモートコマンド50の説明]

監視制御装置3用のリモートコマンド50は、図12に示すように、セキュリティボタン51と、オフボタン52と、伝言記録ボタン53と、伝言再生ボタン54と、メニューボタン55と、上下左右の選択を行なう4個のキーとその中央の決定キーとからなるカーソルボタン56とを備えて構成されている。

【0132】

メニュー項目としては、この例では、管理サーバ装置10に対する電子鍵情報としての個人IDの登録、ドアロック装置2のドアロック制御モードの設定、その他が、用意されており、それぞれのメニュー項目に対応する処理を実行するアプリケーションプログラムは、監視制御装置3のROM203に格納されている。

【0133】

[管理サーバ装置 10 の構成]

次に、管理サーバ装置 10 の構成例を図 17 に示す。管理サーバ装置 10 は、コンピュータの構成を備えており、CPU 301 に対して、システムバス 302 を介して、プログラムやデータが記録されている ROM 303 と、ワークエリア用 RAM 304 と、ドアロック装置管理データベース 305 と、電子鍵登録・紛失履歴メモリ 306 と、インターネットなどの通信ネットワークを通じて通信を行なうための通信インターフェース 307 とが接続されている。また、システムバス 302 には、さらに、ホームページ用メモリ 308 と、画像・音声メモリ 309 とが接続されている。

【0134】

ドアロック装置管理データベース 305 には、ドアロック装置 2 および監視制御装置 3 のシリアル番号、ドアロック装置 2 および監視制御装置 3 が設置された住所、電話番号、IP アドレス、ドアロック装置の利用者の氏名、登録された電子鍵情報を個人プロファイル情報など、ドアロック装置 2 の管理に必要な事項が格納されている。電話番号、IP アドレスは、ドアロック装置 2 および監視制御装置 3 の通信ネットワーク 9 上のアドレス情報である。

【0135】

電子鍵登録・紛失履歴メモリ 306 には、各ドアロック装置 2 ごとに、電子鍵情報の登録と紛失の履歴が記憶される。ホームページ用メモリ 308 には、ホームページの各ページの表示情報が格納されており、CPU 301 の指示に従い、必要がページの表示情報が、このメモリ 308 から読み出されて、通信インターフェース 307 を通じて通信ネットワークに送出される。

【0136】

画像・音声メモリ 309 は、後述するように、セキュリティ監視システムから送られてくる画像・音声情報を格納する。管理サーバ装置 10 では、セキュリティ監視システムからの画像・音声をチェックして、警備会社に通知したり、ユーザの求めに応じて、画像・音声情報をホームページを通じて提供するようにする。

【0137】

次に、以上のような構成の通信システムにおける種々の動作について、以下に説明する。

【0138】

〔監視制御装置3における伝言記録および伝言再生；図18〕

前述したように、この例の監視制御装置3は、電子鍵装置、この例ではICカード40Fと、リモートコマンド50を用いて、特定の家人を指定して、伝言を記録しておくことができる。伝言が監視制御装置3に記録されているときには、LED37が点灯あるいは点滅して、その旨を知らせるようにしている。

【0139】

そして、監視制御装置3に、伝言が記録されている場合には、帰宅した家人が、自分の電子鍵装置としてのICカード40Fを、この電子鍵リード／ライト部36により読み取らせ、リモートコマンド50により伝言再生を指示すると、記録されている伝言が、その人宛ての伝言である場合には、監視制御装置3は、記録されている伝言を、テレビ受像機7やスピーカ35を通じて再生するように構成されている。

【0140】

図18は、この伝言記録および再生のための監視制御装置3の処理を説明するためのフローチャートである。この図18の各ステップSの処理は、CPU201がROM203に記憶されているプログラムにしたがって実行されるものである。

【0141】

すなわち、まず、使用者は、伝言記録または伝言再生をするには、自分のICカード40Fを電子鍵リード／ライト部36にかざして、通信を行なうようにする。CPU201は、電子鍵リード／ライト部36でICカード40Fと通信が行なわれたか否かを判別し（ステップS21）、通信が行われたと判別すると、受信した識別情報により、誰のICカード40Fと通信したかを認識する（ステップS22）。

【0142】

次に、リモートコマンド50からのリモコン信号の到来を待ち（ステップS2

3)、リモコン信号を受信したことを確認したら、そのリモコン信号は、伝言記録ボタン53の操作によるものか否か判別し(ステップS24)、伝言記録ボタン53の操作によるものであると判別したときには、CPU201は、伝言記録動作を行なうようにする(ステップS33)。

【0143】

この伝言記録動作においては、監視制御装置3は、ビデオカメラ31で撮影された伝言者の画像情報をカメラインターフェース210を介して取り込み、画像・音声メモリ208の伝言記録領域に格納すると共に、マイクロホン34で収音した伝言音声情報(伝言メッセージ)をインターフェース218を通じて取り込み、画像・音声メモリ208の伝言記録領域に格納する。このとき、それら画像情報および音声情報は、電子鍵装置40から読み込んだ識別情報に対応付けられて、当該識別情報と共に画像・音声メモリ208に格納される。

【0144】

次に、CPU201は、家族情報メモリ208に記憶されている家族の個人プロフィール情報を参照して、伝言記録をしようとしている操作者以外の伝言相手のリストをテレビ受像機7の画面に表示する(ステップS34)。このとき、テレビ受像機7に電源が投入されていないときには、リモコン送信部38を通じて電源をオンにするリモコン信号をテレビ受像機7に供給して、テレビ受像機7に電源を投入しておく。なお、伝言相手のリストの画面は、例えばスーパーインポーズによりテレビ番組の画像に重ねて表示するようにしてもよいし、テレビ番組の画像に重ねることなく単独の画面としてもよい。

【0145】

操作者は、この伝言相手のリストから、リモートコマンド50のカーソルキー56を用いて、伝言相手の選択入力を行ない、カーソルキー56中の中央の決定キーを押す。監視制御装置3のCPU201は、この伝言相手の選択入力を受信して(ステップS35)、当該伝言相手の情報を、画像・音声メモリ208の伝言記録領域の、前記画像情報および伝言音声メッセージに対応させて格納して登録する(ステップS36)。そして、伝言が記録されたことを報知するために、1個のLED37を点灯させる(ステップS37)。LED37は、図12に示

したように複数個設けられており、記録されている伝言の数だけ、点灯することとなる。

【0146】

また、ステップS24において、リモコン信号が伝言記録ボタン53の操作によるものではないと判別したときには、伝言再生ボタン54の操作によるものであるか否か判別する（ステップS25）。伝言再生ボタン54の操作によるものでないと判別したときには、CPU201は、当該操作されたボタンに応じた処理を行なう（ステップS26）。

【0147】

そして、ステップS25において、伝言再生ボタン54の操作によるものであると判別したときには、CPU21は、ステップS22で認識した識別情報を検索子として、画像・音声メモリ208の伝言記録領域の記憶内容を検索して、ICカード40Fを電子鍵リード／ライト部36にかざした操作者宛ての伝言があるか否か判別する（ステップS27）。

【0148】

そして、ステップS27において、操作者宛ての伝言が無いと判別したときには、CPU201は、例えば予めROM203に用意されている「伝言はありません」の文字情報をテレビ受像機7の画面に表示すると共に、スピーカ35を通じて音声として放音して、操作者に報知する（ステップS28）。

【0149】

また、ステップS27において、操作者宛ての伝言が有ると判別したときには、当該操作者宛ての伝言画像および伝言音声を画像・音声メモリ208から読み出して、テレビ受像機7に表示すると共に、スピーカ35から放音して再生する（ステップS29）。

【0150】

伝言の再生が終了すると、CPU201は、テレビ受像機7の画面に伝言を消去するかどうかの問い合わせを表示するので、操作者は、その表示画面に含まれる「YES」、「NO」のいずれかをリモートコマンド50のカーソルキー56を用いて選択する。CPU201は、当該操作者の選択入力から、伝言を消去す

るか否か判別し（ステップS30）、消去すると判別したときには、画像・音声メモリ208の対応する画像・音声情報を消去し（ステップS31）、点灯しているLED37の一つを消灯する（ステップS32）。そして、この伝言記録再生処理ルーチンを終了する。

【0151】

また、ステップS30で、伝言を消去しないと判別したときには、そのまま、この伝言記録再生処理ルーチンを終了する。

【0152】

[ドアロック制御モードの選択設定；図19、図20]

前述したように、この実施形態では、監視制御装置3を通じてドアロック制御モードの設定ができるようにされているので、その設定動作を、図19のフローチャートを参照しながら説明する。

【0153】

先ず、監視制御装置3のCPU201は、リモコン受信部38の受信信号を監視して、ドアロック制御モードの設定を含む設定メニューのための特定のボタン操作がなされたか否か判別する（ステップS41）。この例では、この特定のボタン操作としては、通常の利用者が行なわない操作とされており、例えばセキュリティボタン51とメニューボタン55との同時操作などとされている。このような特定のボタン操作は、ドアロック装置2の設置業者等が設定作業を行なうために定義されている。簡単に、ドアロック制御モードの設定変更ができないようにするためである。

【0154】

ステップS41で、前記の特定のボタン操作はされないと判別されたときには、単独のボタン操作に応じた処理などの、その他の処理を行なう（ステップS42）。また、ステップS41で、前記の特定のボタン操作がされたと判別されたときには、設定メニューの一覧をテレビ受像機7の画面に、前述の伝言記録再生の場合と同様にして表示するようにする（ステップS43）。

【0155】

この設定メニューの一覧表示に対しては、操作者は、行ないたい設定メニュー

項目の選択をリモートコマンド 50 のカーソルキーを用いて行なう。CPU 201 は、リモコン受信部 38 の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップ S 44）、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップ S 45）。そして、設定項目の決定操作がなされたか否か判別する（ステップ S 46）。また、ステップ S 44 で、メニュー項目の選択操作がなされないと判別したときには、即座にステップ S 46 に進んで設定項目の決定操作がなされたか否か判別する。

【0156】

ステップ S 46 で、設定項目の決定操作がなされないと判別したときには、ステップ S 44 に戻る。また、ステップ S 46 で、設定項目の決定操作がなされたと判別したときには、選択された設定項目はドアロック制御モードの設定であるか否か判別し（ステップ S 47）、そうではなかったときには選択された他の設定項目についての処理ルーチンを実行する（ステップ S 48）。

【0157】

ステップ S 47 で、選択された設定項目はドアロック制御モードの設定であると判別したときには、CPU 201 は、テレビ受像機 7 の画面にオートロックモードと、逐次ロックモードとの選択画面を表示する（ステップ S 49）。操作者は、この選択画面において、いずれかの選択入力をカーソルキー 56 を用いて行なう。

【0158】

そこで、CPU 201 は、リモコン受信部 38 を監視して、オートロックモードが選択されたか否か判別し（ステップ S 50）、オートロックモードが選択されたと判別したときには、ドアロック装置 2 をオートロックモードに設定する設定動作を行なう（ステップ S 51）。

【0159】

すなわち、CPU 201 は、監視制御装置 3 に内蔵の不揮発性メモリ部のドアロック装置 2 のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶すると共に、オートロックモードにする旨の指示をドアロ

ック装置 2 に対して、ドアロック装置通信インターフェース 206 を通じて送る。

【0160】

また、ステップ S50 で、オートロックモードではないと判別したときには、CPU201 は、逐次ロックモードが選択されたと判別して、ドアロック装置 2 を逐次ロックモードにする設定動作を行なう（ステップ S52）。

【0161】

すなわち、CPU201 は、監視制御装置 3 に内蔵の不揮発性メモリ部のドアロック装置 2 のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶すると共に、逐次ロックモードにする旨の指示をドアロック装置 2 に対して、ドアロック装置通信インターフェース 206 を通じて送る。

【0162】

以上で、監視制御装置 3 におけるロック制御モードの設定時の動作は終了となる。

【0163】

次に、ドアロック装置通信インターフェース 206 を通じて送られてきたドアロック制御モードの指示情報を受信したドアロック制御装置 100 の動作について、図 20 のフローチャートを参照して説明する。

【0164】

先ず、ドアロック制御装置 100 の CPU101 は、ドアロック制御モードの設定指示情報を監視制御装置 3 から受け取ったか否か判別し（ステップ S61）、受け取らないときには、その他の処理を行なう（ステップ S62）。

【0165】

ステップ S61 で、ドアロック制御モードの設定指示情報を監視制御装置 3 から受け取ったと判別したときには、CPU101 は、選択指示されたドアロック制御モードは、オートロックモードと逐次ロックモードのいずれであるか判別する（ステップ S63）。

【0166】

ステップ S63 で、選択指示されたドアロック制御モードはオートロックモー

ドであると判別したときには、CPU101は、ドアロック装置2のドアロック制御モードをオートロックモードに設定する処理を行なう（ステップS64）。

【0167】

すなわち、ステップS64においては、ドアロック制御装置100のCPU101は、オートロックモードの設定指示に基づき、ドアロック装置2の内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとの両方をアクティブにし、かつ、プログラムROM13のドアロック制御のアプリケーションを、オートロックモード用のものとするようにする。そして、CPU101は、ドアロック制御装置100が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶する。

【0168】

また、ステップS63で、選択指示されたドアロック制御モードは逐次ロックモードであると判別したときには、CPU101は、ドアロック装置2のドアロック制御モードを逐次ロックモードに設定する処理を行なう（ステップS65）。

【0169】

すなわち、ステップS65においては、ドアロック制御装置100のCPU101は、逐次ロックモードの設定指示に基づき、この例では、ドアロック装置2の内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとの両方をアクティブにし、かつ、プログラムROM13のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、CPU101は、ドアロック制御装置100が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

【0170】

なお、この例では、逐次ロックモードにおいても、内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとの両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部exのみをアクティブにして、内側電子鍵リード／ライト部21inを用いないようにす

することもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

【0171】

次に、オートロックモードと、逐次ロックモードのそれぞれの場合のドアロック装置2の動作について説明する。以下に説明するフローチャートにおける各ステップSの動作は、ドアロック制御装置100のCPU101が主として実行する処理動作である。

【0172】

[オートロックモード；図21～図26]

オートロックモードのときの動作を、図21～図26のフローチャートを参照しながら説明する。このオートロックモードのときには、玄関ドア1は、定常状態では、施錠状態とされる。そして、電子鍵装置40が、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exにかざされて通信が両者の間で行なわれ、識別情報、すなわち、電子鍵情報についての認証がとれたときには、所定時間のみ玄関ドアを開錠し、所定時間後に、自動的に玄関ドア1は施錠状態に戻るように、ドアロック制御装置100により制御されるものである。

【0173】

CPU101は、インターフェース105、106を介して、内側電子鍵リード／ライト部21inおよび外側電子鍵リード／ライト部21exを監視し、電子鍵装置40がかざされて、電子鍵装置40と内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exとの間で通信が行われるのを待つ（ステップS71）。

【0174】

そして、ステップS71において、ICカード40Fがかざされて、リード／ライト部21inまたは21exと通信が行なわれたと判別したときには、CPU101は、識別情報をICカード40Fから受信し、例えばRAM104などに一時的に格納する（ステップS72）。このとき、ドアロック制御装置100

が備える時計回路（図示を省略）の時刻情報が、ICカード40Fに与えられ、制御用IC内42のメモリに書き込まれる。また、内側電子鍵リード／ライト部21i nまたは外側電子鍵リード／ライト部21e xのどちらと通信をしたかの情報として、通信相手のID等が制御用IC42のメモリに書き込まれる。

【0175】

次に、CPU101は、内側電子鍵リード／ライト部21i nまたは外側電子鍵リード／ライト部21e xのどちらでICカード40Fと通信が行われたかを判別する（ステップS73）。その判別結果と、前記の通信の時刻情報とは、家族情報メモリ120の、前記識別情報に対応する家人の記録エリアにも書き込まれ、また、監視制御装置3にも、その家族情報メモリ205に記憶させるために転送される。

【0176】

[内側電子鍵リード／ライト部21i nでの通信の場合；図21～図23]

ステップS73で、ICカード40Fと通信が行われたのが内側電子鍵リード／ライト部21i nであると判別したときには、CPU101は、在宅者が外出する場合であるとして、以下のような処理を行なう。なお、この例では、在宅者が玄関ドア1を開錠し、玄関ドア1を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしている。

【0177】

CPU101は、先ず、家族情報メモリ120に記憶されている識別情報と、ICカード40Fから受信した識別情報とを比較して、家族情報メモリ120に記憶されている電子鍵情報としての識別情報の中に、ICカード40Fから受信した識別情報と一致するものがあるかどうかにより、当該ICカード40Fがドアロック装置2に登録された電子鍵装置であるか否かを判別して、当該ICカード40Fについての認証を行なう（ステップS74）。

【0178】

そして、その認証結果を判別し（ステップS75）、家族情報メモリ120に記憶されている識別情報の中に、ICカード40Fから受信した識別情報と一致

するものがなくて、認証が取れなかったとき（認証NG）であると判別したときには、CPU101は、内側LED駆動部107を駆動して、内側LED22inを赤色で点滅させると共に、内側スピーカ23inから警告音を放音して、認証NGであることをICカード40Fの使用者に報知する（ステップS76）。そして、ドアロック機構28は施錠状態のままとして、ステップS71に戻る。

【0179】

また、ステップS75で、家族情報メモリ120に記憶されている識別情報の中に、ICカード40Fから受信した識別情報と一致するものがあって、認証がOKであると判別したときには、CPU101は、内側LED駆動部107を駆動して、内側LED22inを緑色で1秒間点灯させ、認証OKであることをICカード40Fの使用者に報知する（ステップS77）。このとき、CPU101により、併せて内側スピーカ23inから「認証がとれました」というメッセージを放音させるようにしても良い。

【0180】

そして、このとき、認証がOKであることから、CPU101は、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を開錠状態にし（ステップS78）、内側スピーカ23inから、「ドアロックを解除しました」というメッセージを放音させる（ステップS79）。このとき、内側LED22inを、例えば緑色で点滅させ、ドアロックの解除状態をICカード40Fの使用者に報知するようにしてもよい。

【0181】

このとき、CPU101は、ICカード40Fにより内側から玄関ドア1が開錠されたことを認識していることに基づき、当該ICカード40Fの使用者（在宅者）が外出しようとしていると認識する。そして、監視制御装置3に対して窓の開閉状態についての問い合わせを送る（図22のステップS81）。

【0182】

これに対して、監視制御装置3では、窓センサ6a、6bのセンサ出力をセンサハブ207を通じて取得して、窓の開閉を確認する。つまり、戸締りを確認する。そして、窓の開閉状態についての確認結果をドアロック装置インターフェー

ス 206 を通じてドアロック制御装置 100 に返信するようにする。

【0183】

ドアロック制御装置 100 では、この窓の開閉状態についての確認結果を、通信インターフェース 121 を通じて受信する（ステップ S82）。そして、CPU 101 は、受信した当該確認結果を解析して、窓が開放されているか否か判別する（ステップ S83）。

【0184】

そして、窓が開いていると判別したときには、CPU 101 は、窓が開いていることを内側スピーカ 23 in からの放音音声により警告する（ステップ S84）。また、窓が閉じていると判別したときには、CPU 101 は、戸締りが OK であることを内側スピーカ 23 in からの放音音声により報知する（ステップ S85）。

【0185】

次に、CPU 101 は、ドア開閉センサ 27 のセンサ出力をインターフェース 111 を通じて取り込み、玄関ドア 1 が開けられた否か監視する（ステップ S86）。そして、CPU 101 は、玄関ドア 1 が開けられずに所定時間、例えば 10 秒経過したかどうかを判別し（ステップ S87）、10 秒経過したと判別したときには、玄関ドア 1 を自動的に施錠状態に戻すようにする（ステップ S88）。そして、CPU 101 は、内側 LED 22 in を緑色で点滅して、玄関ドア 1 が施錠状態に戻ったことを報知する（ステップ S89）。

【0186】

また、ステップ S86 で、ステップ S78 での開錠後、10 秒以内に玄関ドア 1 が開かれたと判別したときには、CPU 101 は、ステップ S72 で取り込んだ識別情報で示される在宅者が外出をしたと認識して、当該識別情報を含む個人情報、外出者情報として監視制御装置 3 に転送する（ステップ S90）。

【0187】

その後、CPU 101 は、ドア開閉センサ 27 のセンサ出力を参照して、玄関ドア 1 が閉じられたことを確認し（ステップ S91）、玄関ドア 1 が閉じられた後、所定時間、例えば 3 秒経過したことを確認したら（ステップ S92）、ドア

ロック機構駆動部 112 を駆動制御して、ドアロック機構 28 により玄関ドア 1 を施錠状態に復帰させるようにする (図 23 のステップ S101)。そして、CPU101 は、外側 LED 22ex を緑色で点滅して、玄関ドア 1 が施錠状態に戻ったことを IC カード 40F の使用者に報知する (ステップ S102)。この外側 LED 22ex の緑色点滅は、所定時間、例えば 10 秒間続けられる。

【0188】

その後、CPU101 は、前記所定時間、例えば 10 秒経過したか否か判別し (ステップ S103)、所定時間経過していないと判別したときには、ステップ S71 で通信が行われたと判別された IC カード 40F が、再度、外側電子鍵リード/ライト部 21ex と通信したか否か判別する (ステップ S104)、通信がなされないと判別したときにはステップ S103 に戻る。

【0189】

そして、ステップ S103 で、IC カード 40F と外側電子鍵リード/ライト部 21ex とで通信が行われずに、前記所定時間経過したと判別したときには、CPU101 は、内側電子鍵リード/ライト部 21in に対して IC カード 40F がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図 21 のステップ S71 に戻る。

【0190】

また、ステップ S104 で、玄関ドア施錠復帰後、外側 LED 22ex の緑色点滅が終了する所定時間経過する前に、ステップ S71 において通信が行われたと判別された IC カード 40F と外側電子鍵リード/ライト部 21ex とで通信が行われたと判別すると、ステップ S101～S63 で確認された戸締りを再確認する (ステップ S105)。

【0191】

ステップ S105 で、戸締りが OK であると判別したときには、CPU101 は、通信インターフェース 121 を通じてセキュリティモードをオンにする要求を監視制御装置 3 に送信する (ステップ S106)。

【0192】

この要求に対しては、監視制御装置 3 は、そのときの在宅状況をチェックして

、セキュリティレベルが図15に示したいずれのレベルとなるかを判定する。そして、監視制御装置3は、その判定の結果、セキュリティレベルがレベルDであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置100に返し、セキュリティレベルがレベルD以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置100に返す。

【0193】

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップS107）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップS108）。

【0194】

また、ステップS107で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップS109）。その後、ステップS71に戻る。

【0195】

また、ステップS105で、窓が開いていて戸締りが完了していないと判別したときには、CPU101は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップS110）。そして、その後、ステップS71に戻る。

【0196】

[外側電子鍵リード／ライト部21exでの通信の場合；図24～図26]

ステップS71で、ICカード40Fと通信が行われたのが外側電子鍵リード／ライト部21exであると判別したときには、CPU101は、家人が帰宅した場合あるいはその他の外にいる者の入室要求であるとして、以下のような処理

を行なう。

【0197】

CPU101は、まず、家族情報メモリ120に記憶されている識別情報と、ICカード40Fから受信した識別情報とを比較して、家族情報メモリ120に記憶されている識別情報の中に、ICカード40Fから受信した識別情報と一致するものがあるかどうかにより、当該ICカード40Fがドアロック装置2に登録されたICカード40Fであるか否かを判別して、当該ICカード40Fについての認証を行なう（ステップS121）。

【0198】

そして、その認証結果を判別し（ステップS122）、家族情報メモリ120に記憶されている識別情報の中に、ICカード40Fから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証NG）であると判別したときには、CPU101は、外側LED駆動部108を駆動して、外側LED22exを赤色で点滅させると共に、外側スピーカ23exから警告音を放音して、認証NGであることをICカード40Fの使用者に報知する（ステップS123）。そして、ドアロック機構28は施錠状態のままとして、ステップS71に戻る。

【0199】

また、ステップS122で、家族情報メモリ120に記憶されている識別情報の中に、ICカード40Fから受信した識別情報と一致するものがあって、認証がOKであると判別したときには、CPU101は、外側LED駆動部108を駆動して、外側LED22exを緑色で1秒間点灯させ、認証OKであることをICカード40Fの使用者に報知する（ステップS124）。このとき、CPU101により、合わせて外側スピーカ23exから「認証がとれました」というメッセージを放音させるようにしても良い。

【0200】

そして、このとき、認証がOKであることから、CPU101は、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を開錠状態にし（ステップS125）、外側スピーカ23exから、「ドアロックを解

除しました」というメッセージを放音させる（ステップS126）。このとき、外側LED22exを、例えば緑色で点滅させ、ドアロックの解除状態をICカード40Fの使用者に報知するようにしてもよい。

【0201】

次に、CPU101は、ドア開閉センサ27のセンサ出力をインターフェース111を通じて取り込み、玄関ドア1が開けられた否か監視する（ステップS127）。そして、CPU101は、玄関ドア1が開けられずに所定時間、例えば10秒経過したかどうかを判別し（ステップS128）、10秒経過したと判別したときには、玄関ドア1を自動的に施錠状態に戻すようにする（ステップS129）。そして、CPU101は、外側LED22exを緑色で点滅して、玄関ドア1が施錠状態に戻ったことを報知する（ステップS130）。

【0202】

その後、CPU101は、所定時間、例えば10秒経過したか否か判別し（ステップS131）、所定時間経過していないと判別したときには、ステップS71で通信が行われたと判別された電子鍵装置が外側電子鍵リード／ライト部21exと通信したか否か判別し（ステップS132）、通信がなされないと判別したときにはステップS131に戻る。

【0203】

そして、ステップS131で、電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われずに、所定時間経過したと判別したときには、CPU101は、外側電子鍵リード／ライト部21exに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図21のステップS71に戻る。

【0204】

また、ステップS132で、玄関ドア施錠復帰後、所定時間経過する前に、ステップS71において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われたと判別すると、戸締りを確認する（ステップS133）。

【0205】

このステップS133での戸締りの確認は、前述のステップS121～S123において説明した処理と同様に行なう。つまり、ドアロック制御装置100は、監視制御装置3に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置3から取得する。そして、その問い合わせ結果から、戸締りがOKかどうかを判別する。

【0206】

ステップS133で、戸締りがOKであると判別したときには、CPU101は、通信インターフェース121を通じてセキュリティモードをオンにする要求を監視制御装置3に送信する（ステップS134）。

【0207】

この要求に対しては、監視制御装置3は、そのときの在宅状況をチェックして、セキュリティレベルが図15に示したいずれのレベルとなるかを判定する。そして、監視制御装置3は、その判定の結果、セキュリティレベルがレベルDであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置100に返し、セキュリティレベルがレベルD以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置100に返す。

【0208】

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否かを判別する（ステップS135）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップS136）。

【0209】

また、ステップS135で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップS137）。その後、ステップ

S 7 1に戻る。

【0 2 1 0】

また、ステップS 1 3 3で、窓が開いていて戸締りが完了していないと判別したときには、CPU 1 0 1は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップS 1 3 8）。そして、その後、ステップS 7 1に戻る。

【0 2 1 1】

ステップS 1 3 1～ステップS 1 3 8の処理は、一旦、玄関ドア 1 を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部 2 1 e xに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた者が、もう一度、室内に戻って、内側電子鍵リード／ライト部 2 1 i nに対して電子鍵装置をかざすところからやり直す手間を防止するための処理である。

【0 2 1 2】

すなわち、一旦、玄関ドア 1 を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部 2 1 e xに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた、あるいは失敗した場合に、外側電子鍵リード／ライト部 2 1 e xに電子鍵装置をかざして、玄関ドア 1 を一旦開錠させ、その後、1 0 秒待つて再施錠になった後、1 0 秒以内に、再び、外側電子鍵リード／ライト部 2 1 e xに電子鍵装置をかざすことにより、セキュリティモードをオンにすることができるものである。このようにすれば、セキュリティモードをオンに設定するために、開錠してから室内に入り、内側電子鍵リード／ライト部 2 1 i nに電子鍵装置 4 0をかざすところからやり直す必要がなく、便利である。

【0 2 1 3】

次に、ステップS 1 2 7で、ステップS 1 2 5での開錠後、1 0 秒以内に玄関ドア 1 が開かれたと判別したときには、CPU 1 0 1は、ステップS 7 2で取り込んだ識別情報で示される外出者が帰宅したと認識して、当該識別情報を含む個人情報情報を、帰宅者情報として監視制御装置 3 に転送する（図 2 6 のステップS 1 4 1）。

【0 2 1 4】

その後、CPU101は、ドア開閉センサ27のセンサ出力を参照して、玄関ドア1が閉じられたことを確認し（ステップS142）、玄関ドア1が閉じられた後、所定時間、例えば3秒経過したことを確認したら（ステップS143）、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を施錠状態に復帰させるようにする（ステップS144）。そして、CPU101は、内側LED22inを緑色で点滅して、玄関ドア1が施錠状態に戻ったことを報知する（ステップS145）。

【0215】

その後、CPU101は、帰宅者があったことから在宅状況が変更することに基づき、セキュリティレベルの変更指示を監視制御装置3に送る（ステップS146）。

【0216】

このセキュリティレベルの変更指示を受け取った監視制御装置3では、ステップS141での帰宅者情報による在宅状況の変化を認識し、図15に示した在宅状況とセキュリティレベルとの対応テーブルを参照して、セキュリティレベルの変更の必要があるか否かを判別し、必要があるときには、セキュリティレベルを変更する。そして、監視制御装置3は、セキュリティレベルを変更したかどうかを、ドアロック制御装置100に通知する。

【0217】

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティレベルの変更に関する通知を受け取って（ステップS147）、セキュリティレベルが変更されたか否かを判別する（ステップS148）。

【0218】

そして、ステップS148で、セキュリティモードが変更されたと判別したときには、CPU101は、内側スピーカ23inから、「セキュリティレベルを変更しました」というメッセージを放音する（ステップS149）。そして、ステップS71に戻る。

【0219】

なお、以上の説明では、帰宅者があったときには、ドアロック制御装置100

から、ステップS 146において、監視制御装置3にセキュリティレベルの変更指示を送るようにしたが、監視制御装置3では、ステップS 141での帰宅者情報の転送を受けるので、ドアロック制御装置100からのセキュリティレベルの変更指示を受けなくても、自動的にセキュリティレベルの変更が必要かどうかを判断して、必要である場合には、セキュリティレベルを自動的に変更するようにしても良い。その場合には、セキュリティレベルを変更したときには、その旨をドアロック制御装置100に転送するようにする。

【0220】

[逐次ロックモードの説明；図27～図29]

次に、逐次ロックモードのときの動作を、図27～図29のフローチャートを参照しながら説明する。この逐次ロックモードのときには、ICカード40Cが、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exにかざされて通信が両者の間で行なわれ、電子鍵情報としての識別情報についての認証がとれたときには、そのときの玄関ドア1の開錠あるいは施錠の状態とは逆の状態になるように、ドアロック機構28は、ドアロック制御装置100により制御されるものである。

【0221】

CPU101は、インターフェース105、106を介して、内側電子鍵リード／ライト部21inおよび外側電子鍵リード／ライト部21exを監視し、ICカード40Cがかざされて、ICカード40Cと内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exとの間で通信が行われるのを待つ（ステップS151）。

【0222】

そして、ステップS151において、ICカード40Fがかざされて、ICカード40Fと通信が行なわれたと判別したときには、CPU101は、識別情報をICカード40Fから受信し、例えばRAM104などに一時的に格納する（ステップS152）。このとき、前述と同様に、ICカード40Fには時刻情報等が書き込まれると共に、家族情報メモリ120および監視制御装置3の家族情報メモリ205への時刻情報等の書き込みが行なわれる。

【0223】

内側電子鍵リード／ライト部 21 i n または外側電子鍵リード／ライト部 21 e x のどちらで I C カード 40 F と通信が行われたかを判別する（ステップ S 153）。

【0224】

[内側電子鍵リード／ライト部 21 i n での通信の場合；図 27]

ステップ S 153 で、I C カード 40 F と通信が行われたのが内側電子鍵リード／ライト部 21 i n であると判別したときには、C P U 101 は、在宅者が外出する場合あるいは玄関ドア 1 をセキュリティのために施錠する場合であるとして、以下のような処理を行なう。

【0225】

C P U 101 は、まず、家族情報メモリ 120 に記憶されている識別情報と、I C カード 40 F から受信した識別情報とを比較して、家族情報メモリ 120 に記憶されている識別情報の中に、I C カード 40 F から受信した識別情報と一致するものがあるかどうかにより、当該 I C カード 40 F がドアロック装置 2 に登録された電子鍵装置であるか否かを判別して、当該 I C カード 40 F についての認証を行なう（ステップ S 154）。

【0226】

そして、その認証結果を判別し（ステップ S 155）、家族情報メモリ 120 に記憶されている識別情報の中に、I C カード 40 F から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証 N G）であると判別したときには、C P U 101 は、内側 L E D 駆動部 107 を駆動して、内側 L E D 22 i n を赤色で点滅させると共に、内側スピーカ 23 i n から警告音を放音して、認証 N G であることを I C カード 40 F の使用者に報知する（ステップ S 156）。そして、ドアロック機構 28 は、その前の状態のままとして、ステップ S 151 に戻る。

【0227】

また、ステップ S 155 で、家族情報メモリ 120 に記憶されている識別情報の中に、I C カード 40 F から受信した識別情報と一致するものがあって、認証

がOKであると判別したときには、CPU101は、内側LED駆動部107を駆動して、内側LED22inを緑色で1秒間点灯させ、認証OKであることをICカード40Fの使用者に報知する（ステップS157）。このとき、CPU101により、併せて内側スピーカ23inから「認証がとれました」というメッセージを放音させるようにしても良い。

【0228】

そして、CPU101は、現在のドアロック機構28による玄関ドア1のロック状態は、施錠状態になっているか否か判別する（ステップS158）。このステップS158で、ドアロック機構28による玄関ドア1のロック状態が、開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部112を駆動制御する（ステップS159）。

【0229】

そして、CPU101は、内側LED22inを、例えば緑色で点滅させると共に、内側スピーカ23inから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをICカード40Fの使用者に報知するようにする（ステップS160）。

【0230】

そして、CPU101は、ステップS152で取り込んだ識別情報で示される者が、セキュリティのために施錠をしたと認識して、当該識別情報を含む個人情報を、在宅者情報として監視制御装置3に転送する（ステップS161）。

【0231】

また、ステップS158で、現在のドアロック機構28のロック状態は、施錠状態であると判別したときには、CPU101は、ドアロック機構駆動部112を駆動制御して、ドアロック機構28を開錠状態にし（ステップS162）、内側LED22inを、例えば緑色で点滅させると共に、内側スピーカ23inから、「ドアロックを解除しました」というメッセージを放音させる（ステップS163）。

【0232】

そして、このときには、CPU101は、ステップS152で取り込んだ識別

情報で示される者が、開錠をして外出をしたと認識して、当該識別情報を含む個人情報、外出者情報として監視制御装置 3 に転送する（ステップ S 164）。

【0233】

〔外側電子鍵リード／ライト部 21ex での通信の場合；図 28～図 29〕

ステップ S 153 で、IC カード 40F と通信が行われたのが外側電子鍵リード／ライト部 21ex であると判別したときには、CPU 101 は、家人が帰宅して開錠する場合あるいは家人が外出のため施錠する場合であるとして、以下のような処理を行なう。

【0234】

CPU 101 は、まず、家族情報メモリ 120 に記憶されている識別情報と、IC カード 40F から受信した識別情報とを比較して、家族情報メモリ 120 に記憶されている識別情報の中に、IC カード 40F から受信した識別情報と一致するものがあるかどうかにより、当該 IC カード 40F がドアロック装置 2 に登録された電子鍵装置であるか否かを判別して、当該 IC カード 40F についての認証を行なう（ステップ S 171）。

【0235】

そして、その認証結果を判別し（ステップ S 172）、家族情報メモリ 120 に記憶されている識別情報の中に、IC カード 40F から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証 NG）であると判別したときには、CPU 101 は、外側 LED 駆動部 108 を駆動して、外側 LED 22ex を赤色で点滅させると共に、外側スピーカ 23ex から警告音を放音して、認証 NG であることを IC カード 40F の使用者に報知する（ステップ S 173）。そして、ドアロック機構 28 は施錠状態のままとして、ステップ S 151 に戻る。

【0236】

また、ステップ S 172 で、家族情報メモリ 120 に記憶されている識別情報の中に、IC カード 40F から受信した識別情報と一致するものがあって、認証が OK であると判別したときには、CPU 101 は、外側 LED 駆動部 108 を駆動して、外側 LED 22ex を緑色で 1 秒間点灯させ、認証 OK であることを

ICカード40Fの使用者に報知する(ステップS174)。このとき、CPU101により、併せて外側スピーカ23exから「認証がとれました」というメッセージを放音させるようにしても良い。

【0237】

そして、CPU101は、現在のドアロック機構28のロック状態は、施錠状態になっているか否か判別する(ステップS175)。このステップS175で、現在のドアロック機構28による玄関ドア1のロック状態は、施錠状態であると判別したときには、CPU101は、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を開錠状態にし(ステップS176)、内側LED22inを、例えば緑色で点滅させると共に、内側スピーカ23inから、「ドアロックを解除しました」というメッセージを放音させる(ステップS177)。

【0238】

そして、CPU101は、ステップS152で取り込んだ識別情報で示される者が、帰宅のため開錠をしたと認識して、当該識別情報を含む個人情報を、帰宅者情報として監視制御装置3に転送する(ステップS178)。

【0239】

また、ステップS175で、現在の玄関ドア1のロック状態が開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を施錠状態にする(ステップS179)。

【0240】

そして、CPU101は、内側LED22inを、例えば緑色で点滅させると共に、内側スピーカ23inから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをICカード40Fの使用者に報知するようにする(ステップS180)。

【0241】

そして、CPU101は、ステップS152で取り込んだ識別情報で示される者が、外出のために施錠をしたと認識して、当該識別情報を含む個人情報を、外

出者情報として監視制御装置 3 に転送する（ステップ S 1 8 1）。

【0242】

そして、施錠後、CPU 1 0 1 は、所定時間、例えば 1 0 秒経過したか否か判別し（図 2 9 のステップ S 1 8 2）、所定時間経過していないと判別したときには、ステップ S 1 7 1 で通信が行われたと判別された IC カード 4 0 F が、再度、外側電子鍵リード／ライト部 2 1 e x と通信したか否か判別し（ステップ S 1 8 3）、通信がなされないと判別したときにはステップ S 1 8 2 に戻る。

【0243】

また、ステップ S 1 8 3 で、玄関ドア施錠後、所定時間経過する前に、ステップ S 7 1 において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部 2 1 e x とで通信が行われたと判別すると、戸締りを確認する（ステップ S 1 8 4）。

【0244】

このステップ S 1 8 4 での戸締りの確認は、前述のステップ S 1 0 1 ～ S 1 0 3 において説明した処理と同様に行なう。つまり、ドアロック制御装置 1 0 0 は、監視制御装置 3 に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置 3 から取得する。そして、その問い合わせ結果から、戸締りが OK かどうかを判別する。

【0245】

ステップ S 1 8 4 で、戸締りが OK であると判別したときには、CPU 1 0 1 は、通信インターフェース 1 2 1 を通じてセキュリティモードをオンにする要求を監視制御装置 3 に送信する（ステップ S 1 8 5）。

【0246】

この要求に対しては、監視制御装置 3 は、そのときの在宅状況をチェックして、セキュリティレベルが図 1 5 に示したいずれのレベルとなるかを判定する。そして、監視制御装置 3 は、その判定の結果、セキュリティレベルがレベル D であるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置 1 0 0 に返し、セキュリティレベルがレベル D 以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置 1 0 0 に返す。

【0247】

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップS186）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップS187）。

【0248】

また、ステップS186で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップS188）。その後、ステップS151に戻る。

【0249】

また、ステップS184で、窓が開いていて戸締りが完了していないと判別したときには、CPU101は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップS189）。そして、その後、ステップS171に戻る。

【0250】

[監視制御装置3におけるセキュリティ動作；図30]

上述のようにして、監視制御装置3は、ドアロック制御装置100からの指示を受けてセキュリティモードをオンにするが、リモートコマンド50のセキュリティボタン51を押すことによってもセキュリティモードをオンにすることができる。そして、監視制御装置3のセキュリティモードオン状態は、リモートコマンド50のオフボタン52を操作すると、オフとすることができる。

【0251】

図30は、リモートコマンド50を操作することにより、監視制御装置3のセキュリティモードのオン・オフを制御する動作を説明するためのフローチャート

である。

【0252】

まず、CPU201は、リモートコマンド50からの遠隔操作信号を監視して、リモートコマンド50で操作入力が行なわれたか否かを判別する（ステップS191）。そして、操作入力が行なわれたと判別したときには、CPU201は、操作されたのはセキュリティボタン51であるか否かを判別する（ステップS192）。

【0253】

ステップS192での判別の結果、セキュリティボタン51の操作であると判別したときには、CPU201は、リモコン送信部39から電源オンのリモコン信号をテレビ受像機7のリモコン受信部に送り、テレビ受像機7をオンにする（ステップS193）。

【0254】

そして、CPU201は、ROM203から読み出したデータに基づいて生成した画像情報を、テレビインターフェース217を通じてテレビ受像機7に送り、テレビ受像機7の画面にセキュリティモードオンの確認画面を表示する（ステップS194）。その後、CPU201は、リモコン送信部39からテレビ受像機7の電源をオフするリモコン信号を送出して、テレビ受像機7をオフさせる（ステップS195）。

【0255】

そして、CPU201は、その所定時間、例えば5分経過後（ステップS196）、セキュリティモードをオンにして（ステップS197）、セキュリティ監視動作を実行する（ステップS198）。ステップS196における所定時間は、セキュリティボタン51を操作した使用者が、セキュリティモードオンに設定した後、玄関ドアから退出するまでの時間を考慮した時間とされている。

【0256】

ステップS192において、リモートコマンド50で操作されたボタンがセキュリティボタン51ではないと判別したときには、CPU201は、操作されたのはオフボタン52であるか否かを判別する（ステップS199）。このステップ

S199でオフボタン52ではないと判別したときには、CPU201は、他のボタンが押されたことによる処理を実行する（ステップS200）。

【0257】

ステップS199での判別の結果、オフボタン52であると判別したときには、CPU201は、リモコン送信部39から電源オンのリモコン信号をテレビ受像機7のリモコン受信部に送り、テレビ受像機7をオンにする（ステップS201）。

【0258】

そして、CPU201は、ROM203から読み出したデータに基づいて生成した画像情報を、テレビインターフェース217を通じてテレビ受像機7に送り、テレビ受像機7の画面にセキュリティモードオフの確認画面を表示する（ステップS202）。その後、CPU201は、リモコン送信部39からテレビ受像機7の電源をオフするリモコン信号を送出して、テレビ受像機7をオフさせる（ステップS203）。

【0259】

そして、CPU201は、セキュリティモードをオフにする処理を行なう（ステップS204）。以上で、図30の処理ルーチンは終了となる。

【0260】

[セキュリティモードオンにおける監視動作]

図31および図32は、監視制御装置3において、セキュリティモードオンとされたときの処理動作である。これは、前述のリモートコマンド50でのセキュリティボタン51の操作時に起動されるもので、このときのセキュリティレベルは、レベルAの場合である。なお、ドアロック制御装置100からのセキュリティモードオン指示があったときには、前述したように、在宅者の状況が参酌されてセキュリティレベルが決定され、その決定されたセキュリティレベルでセキュリティモードがオンとされるものである。

【0261】

図31においては、まず、CPU201は、ビデオカメラ31の撮影画像の取り込みを開始する（ステップS211）。このとき、マイクロホン34で収音し

た音声も一緒に取り込みを行なう。前述したように、画像・音声メモリ 208 に設けられるセキュリティモード用の監視情報領域は、リングバッファ形式とされており、この例では、最新の 30 秒分の画像・音声情報が常に画像・音声メモリ 208 に格納されるようにされている。監視カメラ 13 からの撮影画像についても同様にされている。

【0262】

次に、CPU 201 は、センサハブ 207 からの窓センサ 16 a、16 b のセンサ出力と、玄関ドア 1 のドア開閉センサ 27 のセンサ出力の監視を開始するように制御する（ステップ S 212）。さらに、CPU 201 は、火災センサ 4 およびガスセンサ 5 のセンサ出力の監視を開始するように制御する（ステップ S 213）。監視カメラ 13 は、火災センサ 4 やガスセンサ 5 のオン・オフに応じてオン・オフする。

【0263】

次に、CPU 201 は、人感センサ 33 のセンサ出力を監視して、侵入者がいないかどうかチェックする（ステップ S 214）。侵入者なしと判別したときには、窓センサ 16 a、16 b のセンサ出力や、ドア開閉センサ 27 のセンサ出力から、異常を検知したか否かを判別する（図 32 のステップ S 231）。

【0264】

ステップ S 231 で、異常を検知しないと判別したときには、CPU 201 は、火災センサ 4 やガスセンサ 5 のセンサ出力から、異常を検知したか否かを判別する（ステップ S 232）。ステップ S 232 で、異常を検知しないと判別したときには、ステップ S 214 に戻る。

【0265】

そして、ステップ S 214 で、侵入者を人感センサ 33 により検知したと判別したときには、CPU 201 は、照明機構 320 を制御して、照明 32 をオンにする（ステップ S 215）。そして、侵入者の検知時点の 10 秒前から、検知時点の 20 秒後までの 30 秒分の画像・音声情報を、画像・音声メモリ 208 から読み出し、1 回目の画像として、管理サーバ装置 10 に転送する（ステップ S 216）。管理サーバ装置 10 では、この転送されてきた画像・音声情報により、

侵入者を認識して、適切な処置を取ることができる。

【0266】

次に、CPU201は、リモコン送信部39からテレビ受像機7に電源オンのリモコン信号を送り、テレビ受像機7をオンにする（ステップS217）。そして、CPU201は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機7に送り、それら威嚇画像および威嚇音声を出力する（ステップS218）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【0267】

次に、CPU201は、監視制御装置3に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS219）。

【0268】

そして、CPU201は、その後、数秒間隔で、画像・音声メモリ208のリングバッファに格納されている30秒分の画像・音声情報を繰り返し管理サーバ装置10に転送する（ステップS220）。そして、CPU201は、人感センサ33が侵入者を検知しなくなったか否か判別し（ステップS221）、検知しなくなるまで、30秒分の画像・音声情報を管理サーバ装置10に転送する処理作業を継続する。

【0269】

そして、CPU201は、人感センサ33が侵入者を検知しなくなったと判別したときには、30秒分の画像・音声情報の管理サーバ装置10への転送を中止する（ステップS222）。そして、ステップS231に戻って、セキュリティ監視を続ける。

【0270】

また、ステップS231において、異常を検知したと判別したときには、CPU201は、窓センサ6a、6bやドア開閉センサ27の近傍に設置されている監視カメラ13からの検知時点の10秒前から、検知時点の20秒後までの30秒分画像を1回目として、管理サーバ装置10に転送する（ステップS234）

【0271】

そして、CPU201は、リモコン送信部39からテレビ受像機7に電源オンのリモコン信号を送り、テレビ受像機7をオンにする（ステップS235）。そして、CPU201は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機7に送り、それら威嚇画像および威嚇音声を出力する（ステップS236）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【0272】

次に、CPU201は、監視制御装置3に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS237）。

【0273】

そして、CPU201は、その後、数秒間隔で、画像・音声メモリ208のリングバッファに格納されている30秒分の画像・音声情報を繰り返し管理サーバ装置10に転送する（ステップS238）。そして、CPU201は、リモートコマンド50のオフボタン52によるオフ指示を待ち（ステップS239）、オフ指示が有ったときには、セキュリティモードをオフとする。

【0274】

また、ステップS232で、火災センサ4またはガスセンサ5で異常が検知されたと判別したときには、CPU201は、監視制御装置3に設定登録されている、例えば警備会社、消防署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS233）。そして、ステップS239に進む。

【0275】

なお、画像・音声情報を監視制御装置3から受け取った管理サーバ装置10は、Webページにそれらの画像・音声情報を載せる。そこで、監視制御装置3から連絡を受け取った携帯電話の持ち主は、管理サーバ装置10の当該Webページにアクセスして、どのような異常が発生したかを知ることができ、適切な対応処置を講じることが可能になる。

【0276】

[監視制御装置3におけるドアロック制御装置100からの指示による連携；

図33]

監視制御装置3のCPU201は、ドアロック制御装置100から受け取った情報や指示に応じて、図33に示すような連携動作を行なう。なお、この例は、セキュリティレベルの変更は、CPU201が、ドアロック制御装置100からの変更指示を受けて行なうのではなく、ドアロック制御装置100からの個人情報を受け取った結果による在宅状況の変化をチェックして、必要に応じて行なうようにした場合である。

【0277】

すなわち、CPU201は、ドアロック制御装置100からセキュリティモードオンの指示を受け取ったか否か判別する（ステップS241）。受け取らないと判別したときには、CPU201は、その他の処理を行なう（ステップS242）。

【0278】

ステップS241でセキュリティモードオンの指示を受信したと判別したときには、CPU201は、家族情報メモリ205の記憶情報を参照して、在宅状況をチェックする（ステップS243）。そして、図15に示したテーブルを参照して、在宅状況に応じたセキュリティレベルを認識し、セキュリティモードオンにすることが可能であるか否か判別する（ステップS244）。

【0279】

ステップS244で、セキュリティモードオンにすることができないと判別したときには、CPU201は、その旨をドアロック制御装置100に通知する（ステップS245）。

【0280】

一方、ステップS244で、セキュリティモードオンにすることが可能であると判別したときには、セキュリティモードをオンにすることができる旨をドアロック制御装置100に通知し（ステップS246）、所定時間経過するのを待つ（ステップS247）。

【0281】

所定時間経過したことを確認したら、CPU201は、在宅状況に応じたセキュリティレベルでセキュリティモードをオンにする（ステップS248）。そして、セキュリティ監視動作を開始する（ステップS249）。

【0282】

このセキュリティ監視動作中において、ドアロック制御装置100から識別情報を含む個人情報を受信したか否か判別し（ステップS250）、受信しなければステップS249に戻って、セキュリティ監視動作を継続する。ドアロック制御装置100から個人情報を受信したと判別したときには、その結果としての在宅状況の変化をチェックし（ステップS251）、セキュリティレベルの変更が必要であるか判別する（ステップS252）。

【0283】

セキュリティレベルの変更が必要ではないと判別したときには、CPU201は、ステップS249に戻って、セキュリティ監視動作を継続する。また、ステップS252で、セキュリティレベルの変更が必要であると判別したときには、変更の結果、セキュリティモードはオフにすべきものであるか否か判別し（ステップS253）、そうではないときには、在宅状況に応じてセキュリティレベルを変更する（ステップS254）。そして、セキュリティレベルを変更した旨をドアロック制御装置100に通知する（ステップS255）。

【0284】

また、ステップS253で、セキュリティモードはオフにすべきものであると判別したときには、セキュリティモードをオフにし（ステップS256）、その旨をドアロック制御装置100に通知する（ステップS257）。そして、ステップS241に戻る。

【0285】

以上のようにして、この実施形態によれば、非接触の電子鍵装置を用いて、施錠、開錠を行なうので、鍵穴がなく、いわゆるピッキング対策の防犯効果がある。

【0286】

また、電子鍵装置の所有者の生体情報により、電子鍵装置において、当該電子鍵装置の使用が所有者であるか否かについてのチェック（認証）を行ない、認証がOKであるときにのみ、電子鍵情報を送出するようにするので、電子鍵装置を紛失したとしても、所有者以外が電子鍵装置を使用して、ドアロック制御をすることは不可能であるので、セキュリティ上の安全性が非常に高い。

【0287】

また、ドアロック装置2を、オートロックモードと、逐次ロックモードとで使い分けることができるので、使用者が、自分の使い勝手に合わせて、いずれのモードにするかを選択することができて、非常に便利である。

【0288】

また、内側電子鍵リード／ライト部21inを設けて、この内側電子鍵リード／ライト部21inによっても、ドアのロック状態を電子鍵装置により制御することができるので、窓などから侵入した不審者が玄関ドアから退出するのを妨げることができる。

【0289】

また、内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとを設けることにより、これらと電子鍵装置との通信により、家族の入退出の管理をすることが容易である。

【0290】

そのため、ドアロック装置2と、監視制御装置3とを組み合わせることにより、効率的なセキュリティ管理をすることができるようになる。そして、セキュリティモードをドアロック時に設定できるようにしているので、従来は、家の中で設定して、所定時間後に、家の外に出なければならないなどのあわただしさを解消することができる。

【0291】

また、窓の閉め忘れがあったときには、ドアの開閉時に確認されるので、窓の閉め忘れを防止することができる。

【0292】

また、家人の年齢、性別などにより、セキュリティモードのレベルを可変する

ことができるようにしたので、在宅者が弱者である場合にも効果的なセキュリティレベルを設定することができる。また、ドアロックの開錠、施錠に連携して、在宅状況の変化を把握することにより、セキュリティレベルの変更をすることができるというメリットもある。

【0293】

[電子鍵装置の電子鍵情報の登録]

この電子鍵情報としての識別情報の登録が簡単にできることはセキュリティの点で好ましくないので、この例では、この電子鍵情報としての識別情報の登録は、次のようにセキュリティを重視した方法により、例えばドアロック装置2の販売業者あるいは設置業者もしくは使用者により行なわれる。

【0294】

先ず、本鍵情報の登録について説明する。この実施形態においては、前述したように、初期的な本鍵情報となる識別情報を記憶する電子鍵装置は、ICカードとしており、ドアロック装置2の販売業者あるいは設置業者から、ドアロック装置2の各戸への設置に際して、使用者に渡される。

【0295】

この実施形態の場合、ドアロック装置2の各戸への設置前に、当該ドアロック装置2を設置する戸の家族構成員の各人についての個人情報が収集される。そして、当該家族構成員の各人に対して、本鍵情報となる識別情報を記憶するICカードが割り当てられ、それぞれのICカードに記憶される本鍵情報としての識別情報と、前記収集された個人情報とからなる個人プロフィール情報が構成される。

【0296】

そして、設置されるドアロック装置2のシリアル番号等からなる製品番号、設置される住所、電話番号、ドアロック装置を利用する家族構成員の氏名などのユーザ情報と、各家族構成員の前記個人プロフィール情報が、予め管理サーバ装置10のドアロック装置管理データベース305に、記憶される。すなわち、家族構成員それぞれの本鍵情報は、各家族構成員の個人プロフィール情報に含められて予め管理サーバ装置10に登録されている。

【0297】

この際に、ドアロック装置管理データベースにおいては、家族構成員の個人プロフィール情報は、監視制御装置3の通信ネットワーク上のアドレス情報に対応して記憶される。当該アドレス情報としては、前述したように、この例では、電話番号やIPアドレスが用いられる。

【0298】

管理サーバ装置10に登録された本鍵情報および各家族構成員の個人プロフィール情報は、ドアロック装置2の設置業者や販売業者が、ドアロック装置2の設置を完了したときに、管理会社の管理サーバ装置10に初期登録要求をしたときに、管理サーバ装置10から監視制御装置3に転送されることにより、監視制御装置3の家族情報メモリ205に書き込まれて登録される。また、監視制御装置3に登録された情報のうち、少なくとも本鍵情報は、ドアロック制御装置100に転送されることにより、その家族情報メモリ120登録される。

【0299】

図34は、初期登録要求を受けたときの管理サーバ装置10の動作を示すものである。図34の各ステップの動作は、主としてCPU301が主体となっていくものである。

【0300】

まず、CPU301は、初期登録要求を受け付けたか否かを判別する（ステップS261）。この初期登録要求は、ドアロック装置2のシリアル番号等の装置識別情報を伴ったものとされているもので、例えばパーソナルコンピュータなどから通信ネットワークを通じて管理サーバ装置10に送られる場合と、電話等で、初期登録要求を受けたオペレータが図示しない入力手段により入力する場合とがある。

【0301】

CPU301は、この初期登録要求を受け取ると、装置識別情報を検索子として、ドアロック装置データベースを検索し、予め登録されているドアロック装置2および監視制御装置3の通信ネットワーク9上でのアドレス情報を読み出して、初期登録要求を含む発呼をする。つまり、初期登録要求されたドアロック装置

2が接続されている監視制御装置3に対して初期登録要求の発呼を行なう（ステップS262）。

【0302】

このとき、監視制御装置3は、自動応答を行なうので、CPU301は、当該監視制御装置3からの応答を確認して、当該監視制御装置3との間に通信路を形成する（ステップS263）。

【0303】

次に、CPU301は、ドアロック装置2に関連して上述のように管理サーバ装置10のドアロック装置データベース205に記憶している、ドアロック装置が設置された家の家族構成員全員についての本鍵情報を含む個人プロフィール情報を監視制御装置3に送信する（ステップS264）。

【0304】

次に、CPU301は、監視制御装置3に送信すべき情報が全部終了し終わり、監視制御装置3から登録完了通知が到来するのを待ち（ステップS265）、登録完了通知を受け取ったと判別したときには、監視制御装置3との通信路を切断して（ステップS266）、この初期登録の処理ルーチンを終了する。

【0305】

この初期登録要求情報を受け取る監視制御装置3の動作を、図35のフローチャートを参照して説明する。

【0306】

監視制御装置3のCPU201は、管理サーバ装置10からの着信を受信したか否か判別し（ステップS271）、管理サーバ装置10からの着信の受信でなかったと判別したときには、その他の処理を行なう（ステップS272）。

【0307】

管理サーバ装置10からの着信を受信したと判別したときには、CPU201は、その着信に自動応答して管理サーバ装置10との間に通信路を形成する（ステップS273）。そして、受信した着信は初期登録要求であるか否か判別する（ステップS274）。初期登録要求であると判別すると、CPU201は、管理サーバ装置10からの登録情報を待ち、登録情報を受信したら（ステップS2

75)、受信した登録情報を、家族情報メモリ205に書き込む(ステップS276)。

【0308】

そして、家族全員についての登録情報の書き込みが完了したら、管理サーバ装置10に登録完了通知を返送し(ステップS277)、管理サーバ装置10との通信路を切断する(ステップS278)。

【0309】

次に、CPU201は、家族情報メモリ205に書き込んで登録した個人プロフィール情報のうち、少なくとも家族構成員のそれぞれについての本鍵情報である識別情報をドアロック制御装置100に転送する(ステップS279)。ドアロック制御装置100は、この情報を受けて、家族情報メモリ120に受信した本鍵情報を登録する。本鍵情報としての識別情報のほかに、家族構成員についての個人情報の必要なものをも、ドアロック制御装置100に転送するようにしてもよいことは言うまでもない。なお、ドアロック制御装置100での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【0310】

そして、CPU201は、ドアロック制御装置100への本鍵情報および必要は情報の転送の終了を確認すると(ステップS280)、この処理ルーチンを終了する。

【0311】

なお、ステップS274で、初期登録ではないと判別したときには、CPU201は、後述するバックアップ鍵の登録要求であるか否か判別し(ステップS281)、バックアップ鍵の登録要求であると判別したときには、当該バックアップ登録の処理を実行する(ステップS282)。このバックアップ登録の処理については後述する。

【0312】

また、ステップS281でバックアップ登録要求ではないと判別したときには、CPU201は、紛失鍵の抹消要求であるか否か判別する(ステップS283)。そして、紛失鍵の抹消要求でないとは判別したときには、CPU201は、そ

の他の処理を実行し（ステップ S 284）、紛失鍵の抹消要求であると判別したときには、当該抹消要求の処理を実行する（ステップ S 285）。以上で、図 35 の処理を終了する。

【0313】

[バックアップ鍵登録について]

この実施形態においては、管理サーバ装置 10 が備える鍵登録ホームページにアクセスすることにより、バックアップ鍵の登録を行なうことができる。図 36 は、このバックアップ鍵登録の際のシステム構成を説明するための図である。また、図 37 および図 38 は、このときの管理サーバ装置 10 の動作を説明するためのフローチャートである。

【0314】

図 36 に示すように、先ず、電子鍵リード／ライト装置 2001 を備える、あるいは電子鍵リード／ライト装置 2001 が接続されているパーソナルコンピュータ 2002 を用意する。そして、電子鍵リード／ライト装置 2001 にバックアップ鍵として登録したい電子鍵装置 40B、例えば IC カード、携帯電話端末、PDA をセットする。

【0315】

これらの電子鍵装置 40B は、前述した IC カード 40F や 40I と同様に、所有者の指紋や虹彩などの生体情報が登録されたメモリ、生体情報の取得部、電磁誘導アンテナなどからなる通信手段、電子鍵装置ごとに異なるように一元管理された識別情報からなる電子鍵情報が格納されたメモリを備える IC チップを備える。そして、各電子鍵装置 40B の IC チップは、前述と同様に、生体情報取得部からの生体情報についての認証を行なって、認証が取れたときに電磁誘導アンテナなどの通信手段を介して電子鍵情報を送出するようにするものである。

【0316】

次に、パーソナルコンピュータ 2002 からインターネット 2003 を通じて管理サーバ装置 10 の鍵登録ホームページにアクセスする。

【0317】

管理サーバ装置 10 では、この鍵登録ホームページへのアクセスの有無を監視

しており（ステップS301）、アクセスがないときには、その他の処理を行っている（ステップS302）。そして、鍵登録ホームページへのアクセスを受信したときには、CPU301は、鍵登録ホームページの表示情報を送信する（ステップS303）。

【0318】

この鍵登録ホームページは、パーソナルコンピュータ2002の画面に表示される。この画面には、登録者の認証確認用情報の入力を促すメッセージと、入力欄が表示されているので、予め定められたパスワードや顧客ID、ドアロック装置2が設置された住所、電話番号、鍵登録を要求している者の氏名などの必要な認証確認用情報を入力した後、当該認証確認用情報を管理サーバ装置10に送る。

【0319】

管理サーバ装置10では、この認証確認用情報を受信したか否か判別し（ステップS304）、受信したら認証がOKであるか否か判別する（ステップS305）。認証が取れなかったとき（認証NGのとき）には、認証NGを報知する画面をパーソナルコンピュータ2002に送る（ステップS306）。

【0320】

この認証NGを報知する画面では、認証確認用情報の再入力を行うことができると共に、アクセスを中断することもできる。鍵登録者は、いずれかの操作を行うことになる。

【0321】

そこで、管理サーバ装置10のCPU301は、認証確認用の情報を再受信したか否か判別し（ステップS307）、再受信しなかったときには、アクセスが中断されたかどうか判別し（ステップS308）、アクセス中断と判別されなかったときには、ステップS307に戻る。そして、ステップS307で、認証確認用の情報を再受信したと判別したときには、CPU301は、ステップS305に戻って、認証が取れるかどうか判別する。ステップS308で中断であると判別したときには、アクセス切断処理を行なう（ステップS309）。

【0322】

ステップS305において、認証がOKであると判別したときには、CPU301は、バックアップ鍵登録用画面を送信する（図36のステップS311）。このバックアップ鍵登録用画面には、鍵登録ボタンと、アクセス中断ボタンがある。鍵登録者は、いずれかのボタンを操作することになる。鍵登録を行なうときには、鍵登録者は、指紋や虹彩などの生体情報の入力を電子鍵装置40Bに対して行なうと共に、鍵登録ボタンを押す。

【0323】

そして、鍵登録ボタンが押されたときには、パーソナルコンピュータ2002は、バックアップ登録したい電子鍵装置40Bから電子鍵リード／ライト部2001により識別情報を読み取って、バックアップ鍵情報として管理サーバ装置10に送る。

【0324】

そこで、管理サーバ装置10のCPU301は、バックアップ鍵情報を受信したか否か判別し（ステップS312）、受信しなかったときには、アクセスが中断されたかどうか判別し（ステップS313）、アクセス中断と判別されなかったときには、ステップS312に戻る。

【0325】

そして、ステップS313で中断であると判別したときには、アクセス切断処理を行なって（ステップS309）、鍵ホームページを閉じる。また、ステップS312で、バックアップ鍵情報を受信したと判別したときには、CPU301は、ドアロック装置データベース305に、鍵登録要求者のバックアップ鍵情報として、受信した電子鍵情報を登録する（ステップS315）。このとき、電子鍵登録・紛失履歴メモリ306にも、その登録したバックアップ鍵情報と、鍵登録要求者の識別情報とがバックアップ登録履歴として、カレンダー情報および時刻情報と共に書き込まれる。

【0326】

そして、アクセス切断を行なった後（ステップS316）、鍵登録要求者が登録されているドアロック装置2が接続されている監視制御装置3に、バックアップ鍵登録要求の発信を行なう（ステップS317）。監視制御装置3では、この

バックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、CPU301は、当該監視制御装置3との間に通信路を形成する（ステップS318）。

【0327】

次に、CPU301は、鍵登録要求者を識別する情報と、バックアップ鍵情報とを監視制御装置3に送信する（ステップS319）。次に、CPU301は、監視制御装置3に送信すべき情報が全部終了し終わり、監視制御装置3から登録完了通知が到来するのを待ち（ステップS320）、登録完了通知を受け取ったと判別したときには、監視制御装置3との通信路を切断して（ステップS321）、このバックアップ鍵登録の処理ルーチンを終了する。

【0328】

次に、前記ステップS317～ステップS319での送信動作により管理サーバ装置10から送られてくるバックアップ鍵情報を受け取る監視制御装置3の動作を、図39のフローチャートを参照して説明する。この処理ルーチンは、図35におけるステップS282の処理に相当する。

【0329】

監視制御装置3のCPU201は、まず、バックアップ鍵情報と、鍵登録要求者の名前などの識別情報とを受信し（ステップS331）、鍵登録要求者を認識する（ステップS332）。次に、受信したバックアップ鍵情報を、認識した登録要求者のバックアップ鍵情報として、家族情報メモリ205に書き込んで登録する（ステップS333）。

【0330】

このとき、当該鍵登録要求者の個人プロフィール情報の電子鍵登録・紛失履歴エリアに、その登録したバックアップ鍵情報とカレンダー情報および時刻情報とがバックアップ登録履歴として書き込まれる。

【0331】

そして、CPU201は、管理サーバ装置10に、バックアップ鍵情報の登録完了通知を送る（ステップS334）。そして、管理サーバ装置10との通信路を切断する（ステップS335）。

【0332】

次に、CPU201は、家族情報メモリ205に書き込んで登録したバックアップ鍵情報である識別情報を、鍵登録要求者の識別情報と共に、ドアロック制御装置100に転送する（ステップS336）。ドアロック制御装置100は、この情報を受けて、家族情報メモリ120に、受信したバックアップ鍵情報を登録する。そして、CPU201は、ドアロック制御装置100への本鍵情報および必要は情報の転送の終了を確認すると（ステップS337）、この処理ルーチンを終了する。

【0333】

なお、ドアロック制御装置100における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、ステップS336およびステップS337の処理は、行なわなくてもよい。つまり、ドアロック制御装置100には、常に本鍵情報が存在すればよいからである。その場合には、後述する紛失鍵抹消登録の際に、紛失鍵情報の抹消と共に、新たに本鍵情報として使用する、予め監視制御装置3にバックアップ登録されていた鍵情報が、監視制御装置3からドアロック制御装置100に転送されるようにされる。

【0334】

なお、ドアロック制御装置100での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【0335】

なお、以上の電子鍵情報としての識別情報の登録動作は一例であって、例えばパーソナルコンピュータ2002および電子鍵リード／ライト装置2001の代わりに、監視制御装置3を用いて、同様にして管理サーバ装置10にアクセスして、バックアップ鍵を登録するようにしても良い。

【0336】

また、管理サーバ装置10を介することなく、監視制御装置3およびドアロック制御装置100に、電子鍵情報としての識別情報を登録することができるようにしても良い。

【0337】

なお、バックアップ鍵登録の際の鍵登録者の認証のために、本鍵情報を管理サーバ装置に送り、その後、バックアップ鍵登録したい電子鍵装置をセットして登録を行なうようにしてもよい。その場合には、鍵登録者の認証は、本鍵情報により行なうことができるので、上述の例における鍵登録者の認証確認用情報の入力
は不要となる。

【0338】

この例の鍵登録方法によれば、電子鍵装置40Bの所有者本人以外の者が登録
することができないので、セキュリティ上、非常に好ましい。

【0339】

[鍵の紛失対策]

電子鍵装置を紛失してしまった場合には、当該紛失した電子鍵装置の悪意の取得者の利用を防止するため、この実施形態では、電子鍵情報の抹消処理を行なうようにする。図40は、本鍵情報の抹消処理を行なう場合のシステム構成を示す図である。また、図41は、そのときの処理手順を説明するためのフローチャートである。

【0340】

まず、紛失者は、管理会社に対して紛失届を提出する（手順S341）。この紛失届は、電話やメールなどが用いられて行なわれる。この際に、紛失者の本人確認が行なわれ（手順S342）、本人確認がOKであったときに、紛失届が受理される（手順S343）。本人確認は、住所、氏名、年齢、電話番号、パスワード、顧客番号などにより行なわれる。

【0341】

次に、管理会社のオペレータは、管理サーバ装置10に対して紛失鍵の抹消登録の指示入力を行なう。これを受けて、管理サーバ装置10では、紛失鍵の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう（手順S344）。管理サーバ装置10のCPU301は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、電子鍵登録・紛失履歴メモリ306に、その抹消したバックアップ鍵情報と、抹消要求者の識別情報とを、電子鍵抹消履歴として、カレンダー情報および時刻情報と共に書き込む

【0342】

また、管理サーバ装置10のCPU301は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理、抹消履歴の書き込みを完了すると、鍵紛失届を出した者が登録されているドアロック装置2が接続されている監視制御装置3を、データベース305から検索して、自動的に、当該監視制御装置3にアクセスして、紛失鍵の抹消要求を送る（手順S345）。

【0343】

紛失鍵の抹消要求を受信した監視制御装置3は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、監視制御装置3は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、個人プロフィール情報の電子鍵登録・抹消履歴エリアに抹消履歴を書き込み、その後、ドアロック装置2に対して紛失鍵の抹消指示をする。そして、バックアップ鍵が登録されていれば、当該バックアップ鍵の格上げ処理も指示する（手順S346）。

【0344】

ドアロック装置2は、監視制御装置3からの指示に従い、紛失鍵情報の抹消およびバックアップ鍵情報の格上げ処理を実行する（手順S347）。

【0345】

なお、前述もしたように、ドアロック制御装置100における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵は、ドアロック制御装置100には登録されない。その場合には、手順S346では、紛失鍵の抹消指示と共に、監視制御装置3にバックアップ登録されている鍵情報を本鍵情報として、ドアロック制御装置100に送る。

【0346】

そして、その場合、ドアロック制御装置100では、手順S347において、抹消指示を受けた鍵情報を抹消すると共に、その代わりに新たに受信した本鍵情報の登録を行なうことになる。

【0347】

図42を参照して、手順S344および手順S345における管理サーバ装置10の動作を説明する。

【0348】

管理会社のオペレータは、管理サーバ装置10に対して紛失鍵の抹消要求者に関する情報を入力して、紛失鍵の抹消要求を入力する。管理サーバ装置10のCPU301は、この紛失鍵の抹消要求が入力されたか否か判別する（ステップS351）。CPU301は、抹消要求がなければ、その他の処理を行なう（ステップS352）。

【0349】

ステップS351で、紛失鍵の抹消要求が入力されたと判別したときには、CPU301は、ドアロック装置データベース305において抹消要求者および紛失鍵の情報を検索し（ステップS353）、抹消要求者の紛失鍵の情報を抹消すると共に、前述したように、電子鍵登録・紛失履歴メモリ306に紛失者および紛失鍵の情報を書き込む（ステップS354）。

【0350】

次に、CPU301は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップS355）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップS356）。

【0351】

そして、抹消要求者が登録されている監視制御装置3の通信ネットワーク9上のアドレスを、データベース305から検索して（ステップS357）、当該監視制御装置3に紛失鍵の抹消要求の発信を行なう（ステップS358）。ステップS355で、バックアップ鍵情報が登録されていないと判別したときには、ステップS357に即座に進む。

【0352】

監視制御装置3では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、CPU301は、当該監視制御装置3との間に通信路を形成する（ステップS359）。

【0353】

次に、CPU301は、抹消要求者を識別する情報と、抹消すべき紛失鍵の情報とを監視制御装置3に送信する（ステップS360）。次に、CPU301は、監視制御装置3に送信すべき情報が全部終了し終わり、監視制御装置3から抹消完了通知が到来するのを待ち（ステップS361）、抹消完了通知を受け取ったと判別したときには、監視制御装置3との通信路を切断して（ステップS362）、この紛失鍵情報の抹消処理ルーチンを終了する。

【0354】

次に、前記手順S346において、管理サーバ装置10から送られてくる紛失鍵の抹消要求を受け取ったときの監視制御装置3の動作を、図43のフローチャートを参照して説明する。この処理ルーチンは、図35におけるステップS285の処理に相当する。

【0355】

監視制御装置3のCPU201は、まず、紛失鍵情報と、抹消要求者の名前などの識別情報とを受信し（ステップS371）、抹消要求者および紛失鍵情報を認識する（ステップS372）。次に、認識した抹消要求者の紛失鍵情報を、家族情報メモリ205から抹消する（ステップS373）。そして、抹消要求者の個人プロフィール情報中の電子鍵登録・抹消履歴情報として、抹消した電子鍵情報としての識別情報および日付、時刻等を、家族情報メモリ205に書き込んだ後、管理サーバ装置10に、抹消完了通知を送る（ステップS374）。そして、管理サーバ装置10との通信路を切断する（ステップS375）。

【0356】

次に、CPU201は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップS376）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップS377）。そして、ドアロック制御装置100に紛失鍵の抹消指示を送る（ステップS378）。ステップS376で、バックアップ鍵情報が登録されていないと判別したときには、ステップS378に即座に進む。

【0357】

ドアロック制御装置100では、抹消指示に従って、紛失鍵情報の抹消を実行した後、抹消完了通知を監視制御装置3に送る。そこで、監視制御装置3は、抹消完了通知の受信を待って（ステップS379）、この処理ルーチンを終了する。

【0358】

なお、ドアロック制御装置100における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵情報が存在するときには、ステップS378では、紛失鍵の情報と共に、本鍵情報に格上げするバックアップ鍵情報を送るようにする。本鍵情報に格上げするバックアップ鍵情報は、抹消完了の後に、監視制御装置3から、ドアロック制御装置100に送るようにしてもよい。

【0359】

なお、ドアロック制御装置100での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【0360】

図41～図43の例では、管理サーバ装置10では、紛失鍵の登録抹消は、まず、管理サーバ装置10で行なった後、監視制御装置3およびドアロック制御装置100で行なわすようにしたが、通信ネットワーク9における支障などによって、監視制御装置3およびドアロック制御装置2における紛失鍵の抹消処理が遅れることがある。

【0361】

しかし、紛失鍵の登録抹消は、セキュリティ管理上では、監視制御装置3およびドアロック制御装置2での登録抹消が早い方がよい。また、管理サーバ装置10の登録内容と、監視制御装置3およびドアロック制御装置2での登録内容とは、できるだけ同一にしておくほうが管理上、好ましい。

【0362】

次に説明する紛失鍵の登録抹消処理手順は、以上の点を考慮したものである。

【0363】

図 4 4 は、その場合における本鍵情報の抹消処理を行なう場合の処理手順を説明するためのフローチャートである。

【0364】

まず、紛失者は、管理会社に対して紛失届を提出する（手順 S 3 8 1）。この紛失届は、電話やメールなどが用いられて行なわれる。この際に、紛失者の本人確認が行なわれ（手順 S 3 8 2）、本人確認が OK であったときに、紛失届が受理される（手順 S 3 8 3）。本人確認は、住所、氏名、年齢、電話番号、パスワード、顧客番号などにより行なわれる。

【0365】

次に、管理会社のオペレータは、管理サーバ装置 1 0 に対して紛失鍵の抹消登録の指示入力を行なう。これを受けて、管理サーバ装置 1 0 は、紛失鍵情報が登録されている監視制御装置 3 およびドアロック制御装置 2 のアドレスを、データベース 3 0 5 から検索して、検索結果の監視制御装置に対して、紛失鍵の抹消要求を送る（手順 3 8 4）。

【0366】

紛失鍵の抹消要求を受信した監視制御装置 3 は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、監視制御装置 3 は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、個人プロフィール情報の電子鍵登録・抹消履歴エリアに抹消履歴を書き込み、その後、ドアロック装置 2 に対して紛失鍵の抹消指示をする。そして、バックアップ鍵が登録されていれば、当該バックアップ鍵の格上げ処理も指示する（手順 S 3 8 5）。

【0367】

ドアロック装置 2 は、監視制御装置 3 からの指示に従い、紛失鍵情報の抹消およびバックアップ鍵情報の格上げ処理を実行し、抹消完了通知を監視制御装置 3 に返送する（手順 S 3 8 6）。

【0368】

このドアロック装置 2 からの抹消完了通知を受けた監視制御装置 3 は、抹消完了通知を管理サーバ装置 1 0 に返送する（手順 S 3 8 7）。

【0369】

抹消完了通知を受けた管理サーバ装置10は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、管理サーバ装置10のCPU301は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、電子鍵登録・紛失履歴メモリ306に、その抹消したバックアップ鍵情報と、抹消要求者の識別情報とを、電子鍵抹消履歴として、カレンダー情報および時刻情報と共に書き込む（手順S388）。

【0370】

なお、前述もしたように、ドアロック制御装置100における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵は、ドアロック制御装置100には登録されない。その場合には、手順S385では、紛失鍵の抹消指示と共に、監視制御装置3にバックアップ登録されている鍵情報を本鍵情報として、ドアロック制御装置100に送る。

【0371】

そして、その場合、ドアロック制御装置100では、手順S386において、抹消指示を受けた鍵情報を抹消すると共に、その代わりに新たに受信した本鍵情報の登録を行なうことになる。

【0372】

図45を参照して、この例の場合における管理サーバ装置10の動作を説明する。

【0373】

管理会社のオペレータは、管理サーバ装置10に対して紛失鍵の抹消要求者に関する情報を入力して、紛失鍵の抹消要求を入力する。管理サーバ装置10のCPU301は、この紛失鍵の抹消要求が入力されたか否か判別する（ステップS391）。CPU301は、抹消要求がなければ、その他の処理を行なう（ステップS392）。

【0374】

ステップS391で、紛失鍵の抹消要求が入力されたと判別したときには、CPU301は、ドアロック装置データベース305において抹消要求者および紛

失鍵の情報および監視制御装置3およびドアロック装置2のアドレスを検索し（ステップS393）、検索した監視制御装置3に対して通信ネットワーク9を通じて、紛失鍵の抹消要求を送る（ステップS394）。

【0375】

監視制御装置3では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、CPU301は、当該監視制御装置3との間に通信路を形成する（ステップS395）。

【0376】

次に、CPU301は、抹消要求者を識別する情報と、抹消すべき紛失鍵の情報とを監視制御装置3に送信する（ステップS396）。次に、CPU301は、監視制御装置3に送信すべき情報が全部終了し終わり、監視制御装置3から抹消完了通知が到来するのを待つ（ステップS397）。

【0377】

そして、ステップS397で、抹消完了通知を受け取ったと判別したときには、監視制御装置3との通信路を切断し（ステップS398）、抹消要求者の紛失鍵の情報を抹消すると共に、前述したように、電子鍵登録・紛失履歴メモリ306に紛失者および紛失鍵の情報を書き込む（ステップS399）。

【0378】

次に、CPU301は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップS400）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップS401）。そして、この紛失鍵情報の抹消処理ルーチンを終了する。

【0379】

[他の実施形態]

上述の実施形態は、セキュリティ監視システムも含む通信システムの構成であったので、管理サーバ装置10が存在しているが、セキュリティ監視システムが存在しない通信システムの構成も可能である。

【0380】

その場合には、監視制御装置 3 で行なえる機能に、バックアップ鍵登録や紛失鍵抹消を用意する。そして、リモートコマンド 50 により、メニューからそれらの機能を選択して、バックアップ鍵登録や、紛失鍵の抹消を行なうようにする。

【0381】

例えば、バックアップ鍵情報の登録は、リモートコマンド 50 により、メニューからバックアップ鍵登録を選択し、監視制御装置 3 に対して、バックアップ鍵情報を登録したい電子鍵装置をかざし、リモートコマンド 50 により、登録要求者の入力を行ない、登録実行を選択することにより、行なうことができる。

【0382】

鍵情報の抹消も同様にして、監視制御装置 3 において行なうことができる。この例の場合にも、監視制御装置 3 からドアロック制御装置 100 に鍵情報を転送したり、抹消指示をしたりするのは、上述の場合と同様である。

【0383】

また、ドアの施錠および開錠のみを目的とするドアロック制御システムとして考えた場合には、監視制御装置 3 は不要である。その場合には、ドアロック制御装置 100 に対して、バックアップ鍵情報の登録を行なったり、紛失鍵情報の抹消を行なったりすることができる構成とすればよい。

【0384】

なお、電子鍵情報は、管理サーバ装置からドアロック装置の電子鍵情報の記憶部に転送して、登録するのではなく、住戸に設置する前に、予め、ドアロック装置に登録して記憶しておくようにしても勿論よい。特に、上述の実施形態のようなセキュリティ監視システムを用いずに、ドアロック制御システムを単独で使用するような場合には、そのようにするものである。

【0385】

上述の例では、バックアップ鍵情報が登録されていても、本鍵情報のみを電子鍵装置からの識別情報の受信時の認証用としたが、家族情報メモリ 120 または 205 に登録されているバックアップ鍵情報をも含む全てを認証用として、常時、用いるようにしても勿論よい。

【0386】

その場合には、鍵紛失による抹消は、当該鍵情報の抹消を行なうだけでよく、上述の例のように、バックアップ鍵を本鍵情報に格上げするようにする処理は不要となる。

【0387】

なお、上述の実施形態では、本鍵情報は、予め管理サーバ装置にドアロック装置の設置会社や販売会社などにより、登録しておくようにしたが、本鍵情報もバックアップ情報と同様にして、上述のようにして後から登録することができるようにしてもよい。

【0388】

また、上述の実施形態では、パーソナルコンピュータを用いてバックアップ鍵の登録を行なうようにしたが、監視制御装置3から管理サーバ装置10にアクセスすることにより、行なうこともできる。その場合には、監視制御装置3が備える電子鍵リード／ライト部36を利用することができるので、電子鍵リード／ライト装置を別個に用意する必要はない。

【0389】

また、パーソナルコンピュータの代わりに、電子鍵リード／ライト装置に接続される携帯電話端末から、管理サーバ装置のホームページにアクセスして、バックアップ鍵登録を行なうようにすることもできる。

【0390】

また、上述の実施形態では、電子鍵情報の紛失届による抹消は、本鍵情報について説明したが、紛失届の際に、本鍵情報の紛失届か、バックアップ鍵情報の紛失届かの指定をすることにより、バックアップ鍵情報の紛失届およびそれに基づくバックアップ鍵情報の抹消処理をすることもできる。

【0391】

また、ICチップのメモリには、予め一元管理された識別情報が記憶されているように説明したが、後から、一元管理されている識別情報が書き込まれるようにされてもよいことは言うまでもない。

【0392】

なお、上述の実施形態では、電子鍵装置を、外側電子鍵リード／ライト部21

ex に対して、ドアの施錠後、所定時間以内にかざした場合に、セキュリティモードをオンにするようにしたが、ドアロック制御装置 100 または監視制御装置 3 では、玄関ドア 1 からの入退出を管理しているので、在宅者が無くなったら、自動的にセキュリティレベル A でセキュリティモードをオンにするようにすることもできる。

【0393】

その場合に、ドアロック制御装置 100 で、在宅者無しを検出したときに、監視制御装置 3 にセキュリティモードオンを要求しても良いし、監視制御装置 3 が、自装置で、在宅者無しを検出したときに、セキュリティモードオンとするようにしても良い。

【0394】

なお、この例では、在宅者が玄関ドア 1 を開錠し、玄関ドア 1 を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしたが、セキュリティモードがオンになっているときに外出者があった場合には、外出者を電子鍵装置との通信により取得される識別情報により認識して、監視制御装置 3 が、帰宅者があった場合と全く同様に、在宅状況の変化に対応して自動的にセキュリティレベルを変更するようにすることもできる。

【0395】

なお、以上の実施形態の説明では、鍵情報としての識別情報の認証は、ドアロック装置で行なうようにしたが、ドアロック装置 2 は、監視制御装置 3 に、あるいは監視制御装置 3 を介して管理サーバ装置 10 に鍵情報を送り、監視制御装置 3 あるいは管理サーバ装置 10 で、認証作業を行ない、その認証結果を、ドアロック装置 2 に返す（管理サーバ装置 10 の場合には監視制御装置 3 を介して返す）ようにしても良い。その場合には、監視制御装置 3 からドアロック制御装置 100 への鍵情報の転送や抹消指示を送る必要はない。

【0396】

また、開錠者、施錠者の識別情報も監視制御装置 3 ではなく、管理サーバ装置 10 に送り、管理サーバ装置 10 により、セキュリティ管理をするようにしても

よい。

【0397】

また、以上の説明では、外出者か帰宅者かは、ドアロック制御装置100で判別するようにしたが、監視制御装置3においても、ドアロック制御装置100でのドアロック制御モードの設定情報を備えているので、ドアロック制御装置100は、ICカード40Fが、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exにかざされて通信が両者の間で行なわれ、識別情報についての認証がとれたときには、その識別情報と、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exのいずれと通信したかの情報と、開錠か施錠かの情報とを、監視制御装置3に送り、監視制御装置3が、外出か帰宅かを判別するようにすることもできる。

【0398】

なお、一つのドアロック装置に一つの電子鍵情報として、当該家に住む家族構成員の全員に共通の一つの電子鍵情報を用いるようにして、各人が、その共通鍵情報を格納する電子鍵装置をそれぞれ持つようにすることもできる。

【0399】

また、電子鍵装置は、上述の実施形態のような非接触形式で電子鍵情報の通信を行なうのものに限られるものではなく、接触形式で電子鍵情報の通信を行なうものであっても勿論よい。

【0400】

【発明の効果】

以上説明したように、この発明によれば、予め登録された所有者の生体情報が確認されたときにのみ、電子鍵情報を送出するように制御することができるので、当該電子鍵装置を紛失したとしても、電子鍵装置の電子鍵情報記憶部に登録された生体情報と一致しない悪意の拾得者の使用を阻止することができるものである。

【0401】

そして、電子鍵情報として、同一のものが存在しないように一元管理されて割り振られた識別情報を用いた場合には、個人の生体情報が確認されたときにのみ

、電子鍵情報を送出するように制御することができるので、電子鍵情報は、個人識別情報として使用することができる。

【図面の簡単な説明】

【図 1】

この発明のドアロック制御システムの実施の形態で用いる識別情報の概要を説明するための図である。

【図 2】

この発明の実施形態で用いる識別情報の一例を示す図である。

【図 3】

この発明によるドアロック制御システムの実施形態が適用された通信システムの概要を説明するための図である。

【図 4】

この発明による電子鍵装置の一実施形態を示す図である。

【図 5】

この発明による電子鍵装置の一実施形態の構成例を示すブロック図である。

【図 6】

この発明による電子鍵装置の一実施形態の動作を説明するためのフローチャートである。

【図 7】

この発明による電子鍵装置の他の実施形態を示す図である。

【図 8】

この発明による電子鍵装置の他の実施形態の構成例を示すブロック図である。

【図 9】

この発明による電子鍵装置の他の実施形態の動作を説明するためのフローチャートである。

【図 10】

実施形態のドアロック制御システムを構成するドアロック装置の一例の要部を説明するための図である。

【図 11】

図10のドアロック装置のドアロック制御装置の構成例を示すブロック図である。

【図12】

セキュリティシステムに用いる監視制御装置の例を示す図である。

【図13】

図12の監視制御装置の構成例を示すブロック図である。

【図14】

個人プロフィール情報の一例を示す図である。

【図15】

セキュリティモードの内容を説明するための図である。

【図16】

セキュリティモードの内容を説明するための図である。

【図17】

管理サーバ装置の構成例を示すブロック図である。

【図18】

図12の監視制御装置の伝言記録および再生機能を説明するためのフローチャートである。

【図19】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図20】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図21】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図22】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図23】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制

御動作を説明するためのフローチャートの一部である。

【図 2 4】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 5】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 6】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 7】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 8】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 9】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 3 0】

監視制御装置のリモートコマンドからの信号の受信処理動作を説明するためのフローチャートである。

【図 3 1】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図 3 2】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図 3 3】

監視制御装置におけるドアロック装置との連携動作を説明するための図である。

【図 3 4】

この発明における実施形態において、本鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 5】

この発明における実施形態において、本鍵情報の登録を説明するためのシステム構成を示す図である。

【図 3 6】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのシステム構成を示す図である。

【図 3 7】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 8】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 9】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図 4 0】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合のシステム構成を説明するための図である。

【図 4 1】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合の手順の一例を説明するための図である。

【図 4 2】

図 4 1 の例における紛失鍵情報の抹消処理を説明するためのフローチャートを示す図である。

【図 4 3】

図 4 1 の例における紛失鍵情報の抹消を説明するためのフローチャートを示す図である。

【図 4 4】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合の手順の他の例を説明するための図である。

【図 4 5】

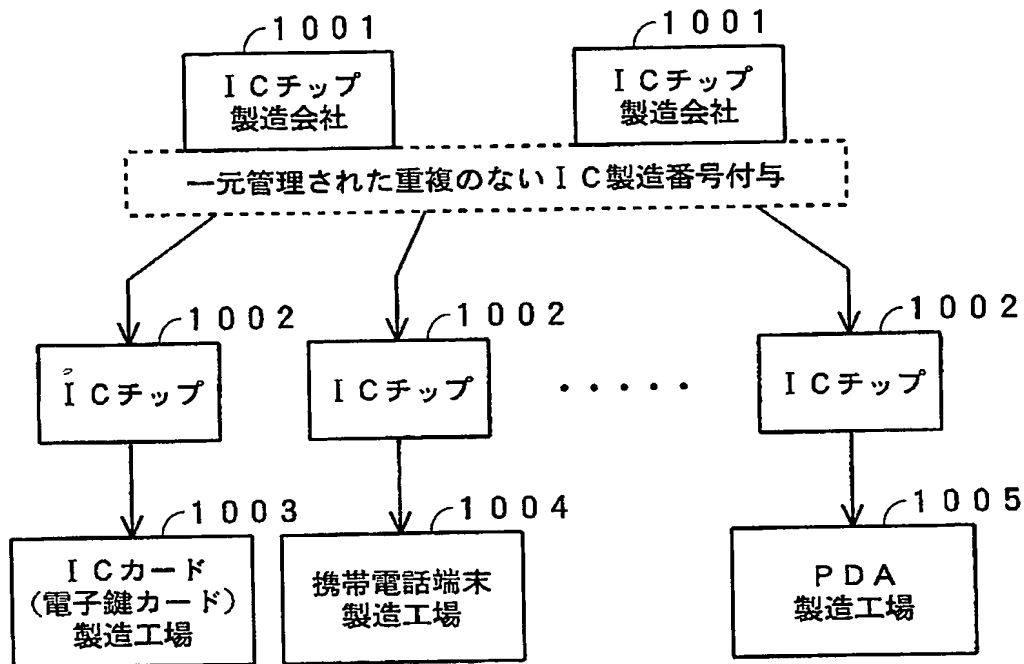
図 4 4 の例における紛失鍵情報の抹消処理を説明するためのフローチャートを示す図である。

【符号の説明】

1…玄関ドア、2…ドアロック装置、3…監視制御装置、4…火災センサ、5…ガスセンサ、6 a, 6 b…窓センサ、7…テレビ受像機、8…電話回線、10…管理サーバ装置、100…ドアロック制御装置、21 i n…内側電子鍵リード／ライト部、21 e x…外側電子鍵リード／ライト部、40 F、40 I…電子鍵装置の例としての I C カード

【書類名】 図面

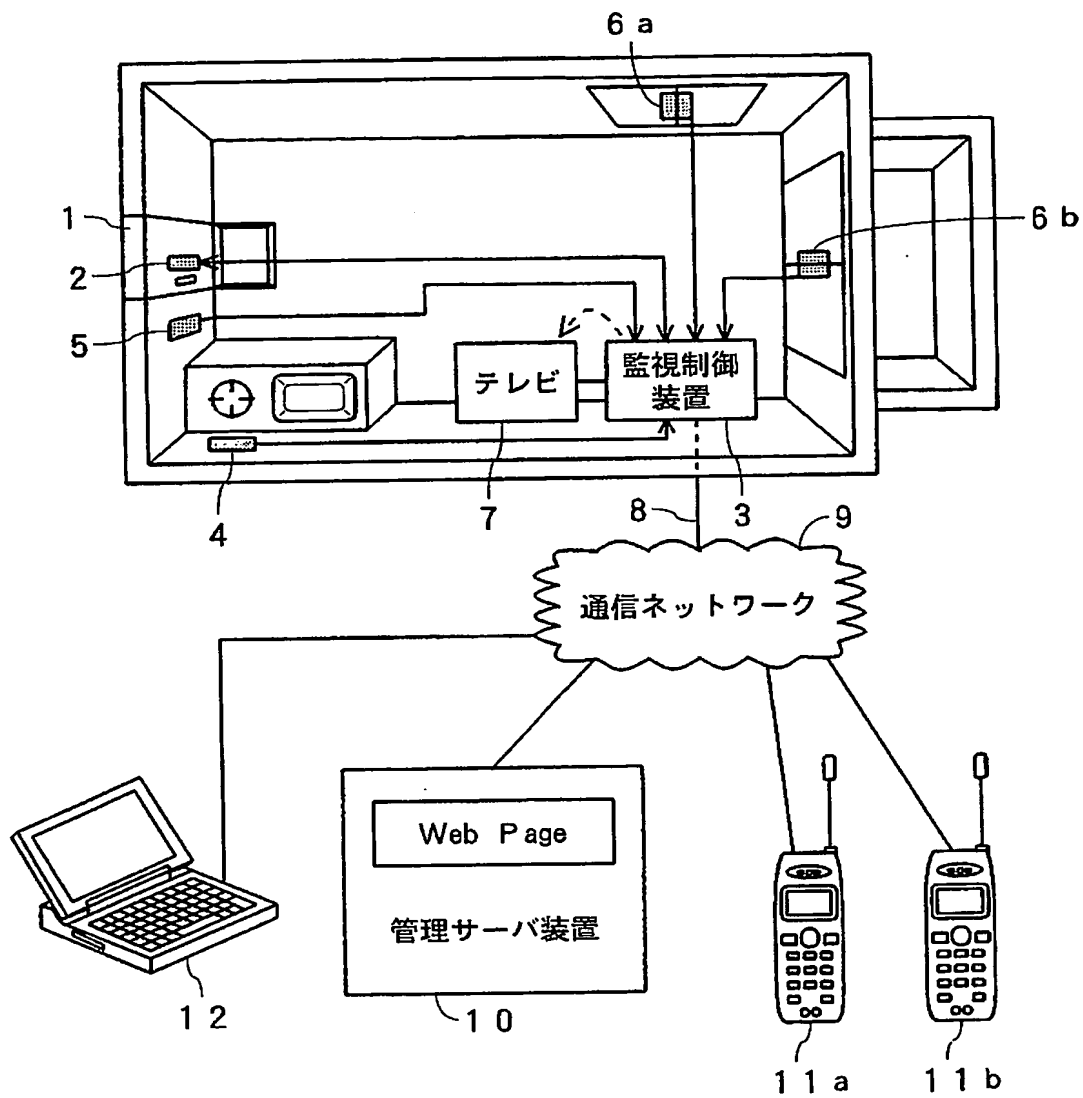
【図 1】



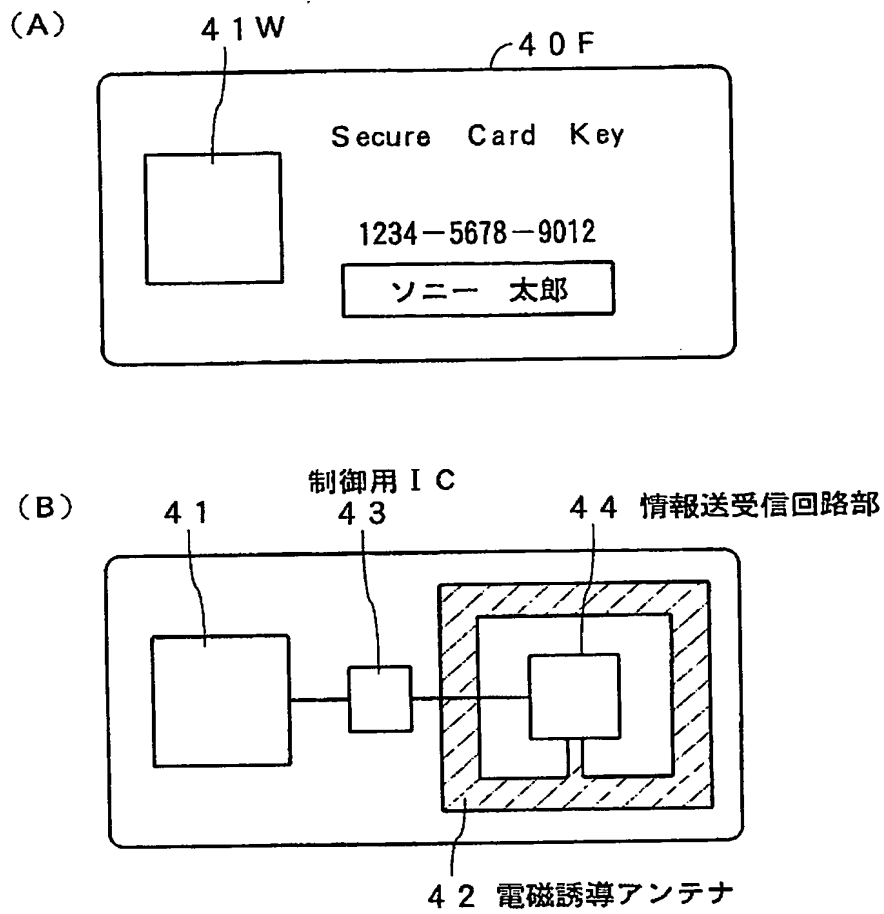
【図 2】

| | | |
|------------|-------------|------------|
| 00 | AKKK | 0001 |
| メーカー 番号 | カテゴリ コード | シリアル 番号 |

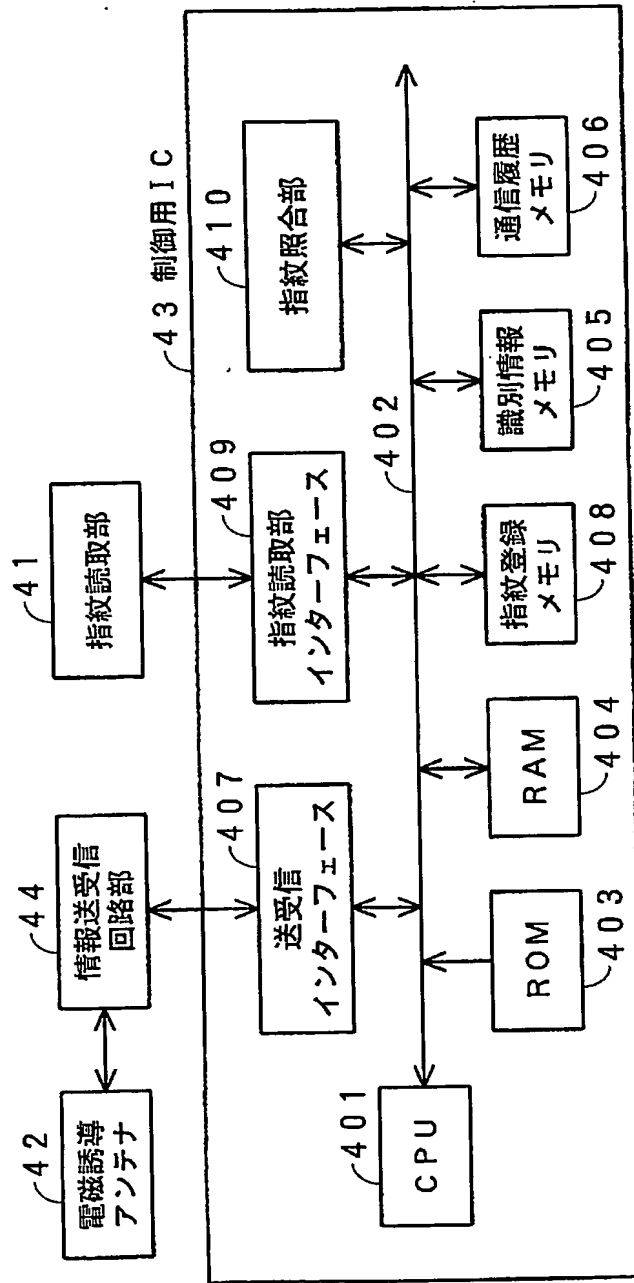
【図 3】



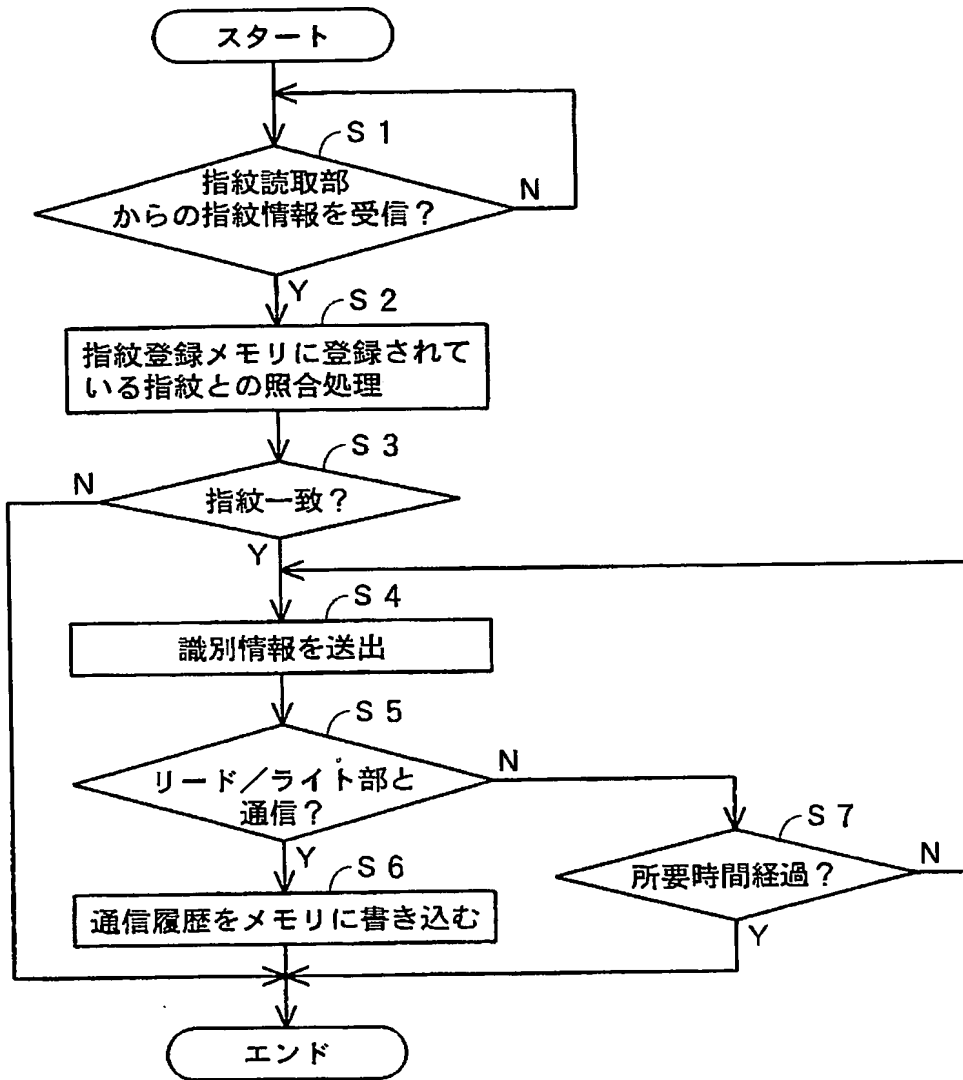
【図 4】



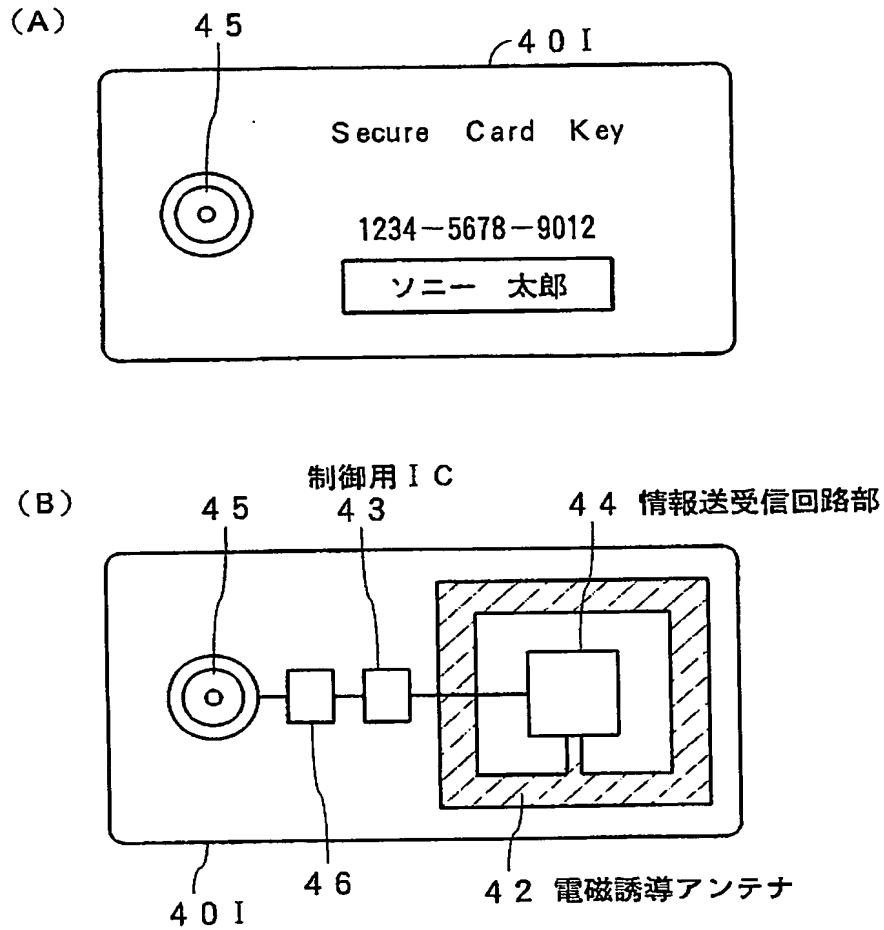
【図 5】



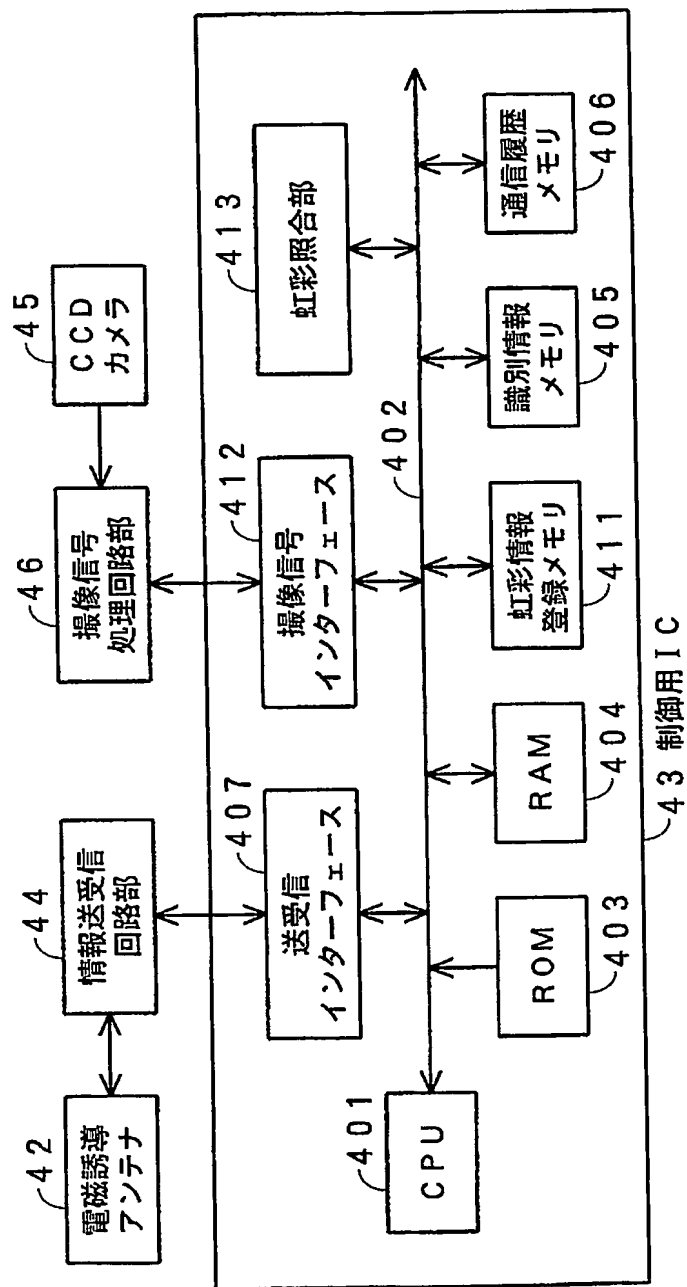
【図 6】



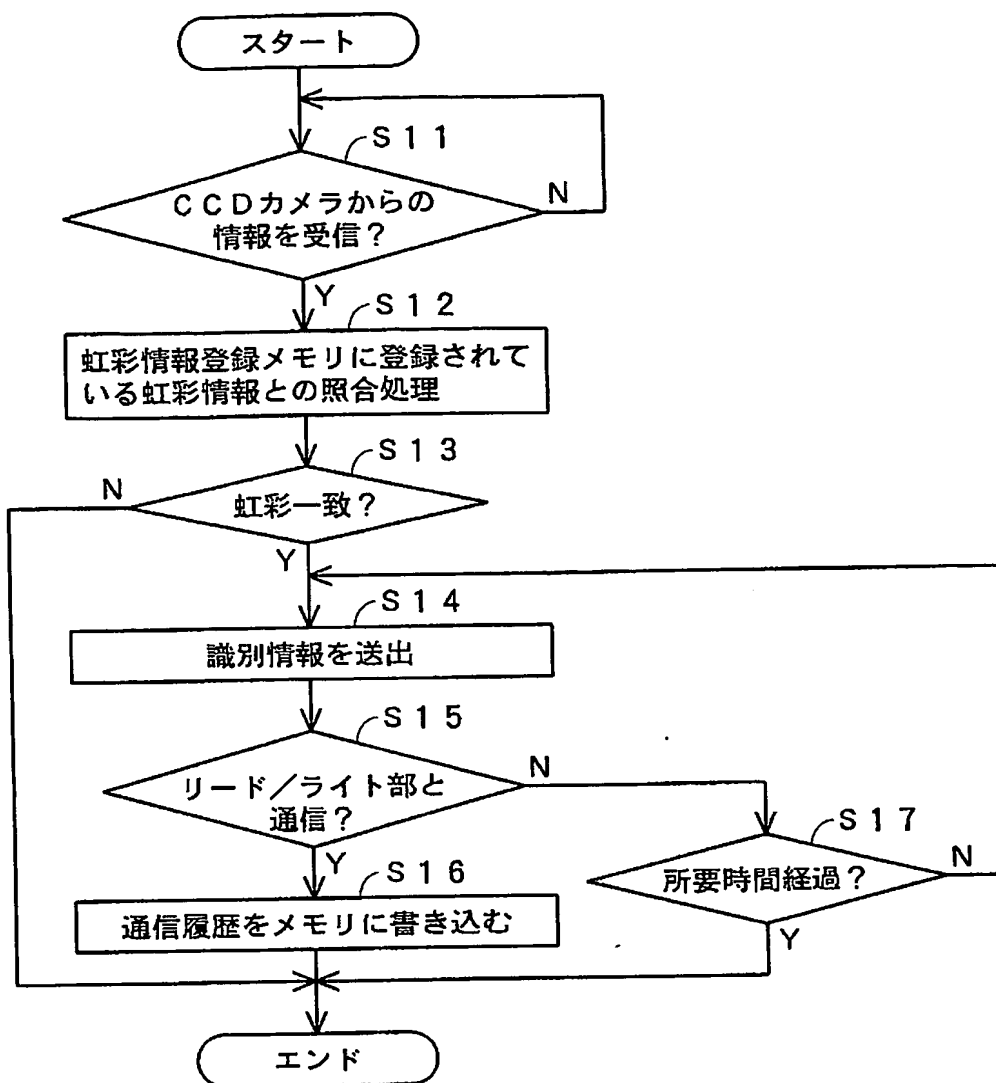
【図 7】



【図 8】

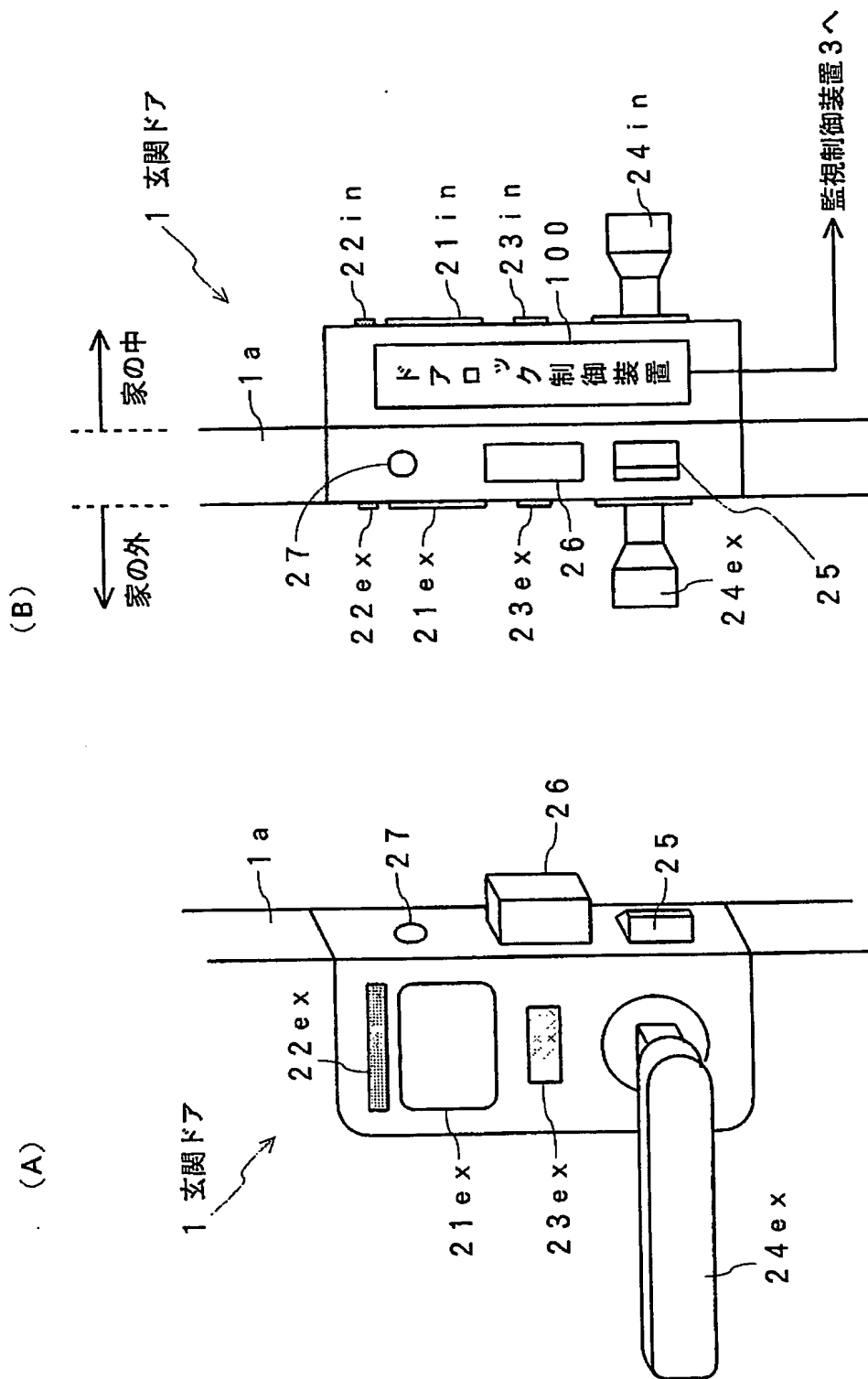


【図9】



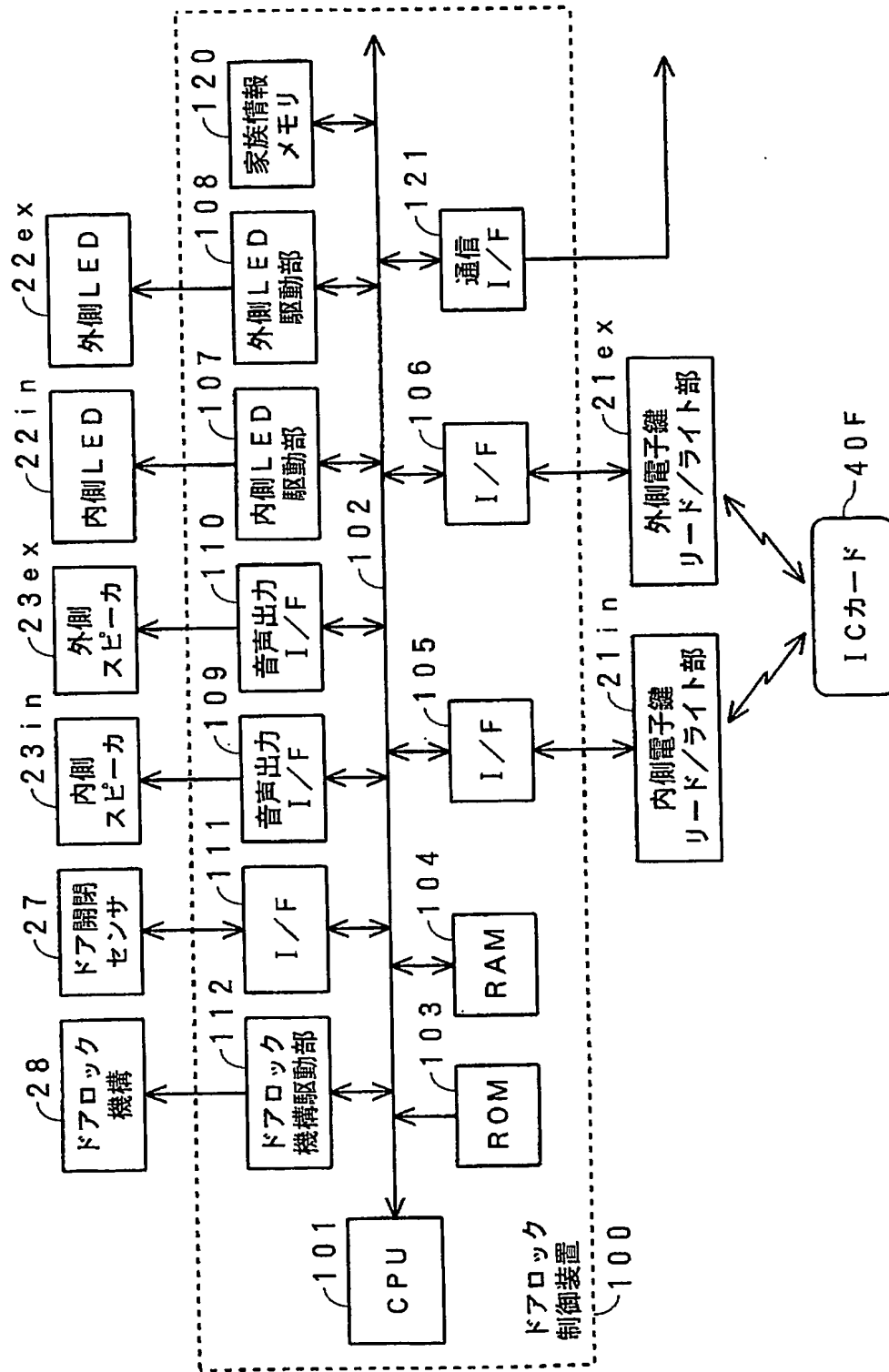
【図10】

2 ドアロック装置



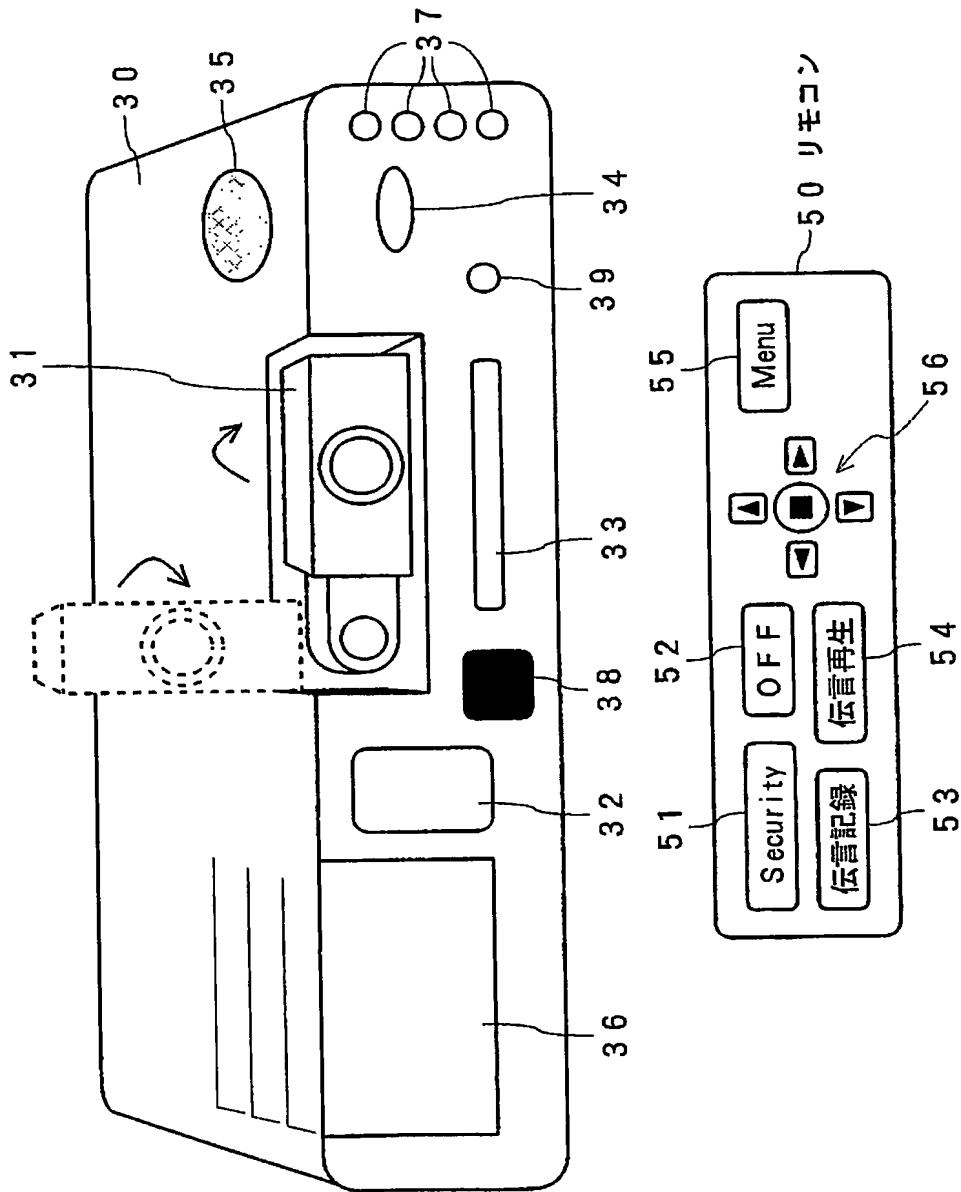
【図 1 1】

2 ドアロック装置

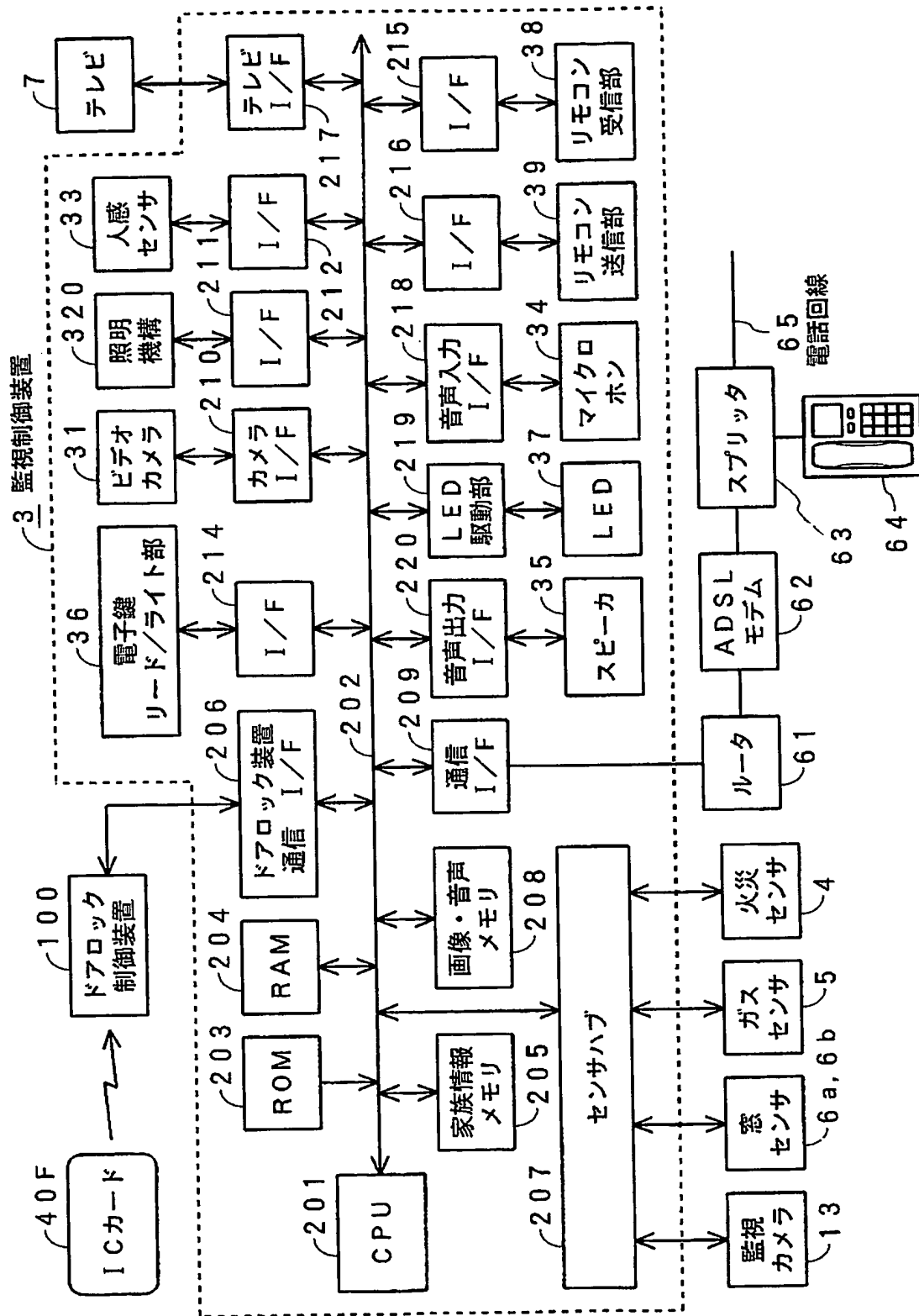


【図12】

3 監視制御装置



【図13】



【図 14】

個人プロフィール情報

| | | |
|--|--|--------|
| | 識別情報 ・本鍵情報 ・バックアップ鍵情報 | 個人識別情報 |
| | パスワード情報 | |
| | 氏名 | |
| | 住所 | |
| | 生年月日 | |
| | 年齢 | |
| | 続柄 | |
| | 登録日 | |
| | 銀行口座番号 | 個人情報 |
| | 電話番号 | |
| | I P アドレス | |
| | 趣味／嗜好情報 ・好きなテレビ番組：ドラマ ・好きな音楽：ジャズ ・好きな映画：S F | |
| | 入退出履歴情報 | |
| | 電子鍵登録・紛失履歴情報 | |

【図 15】

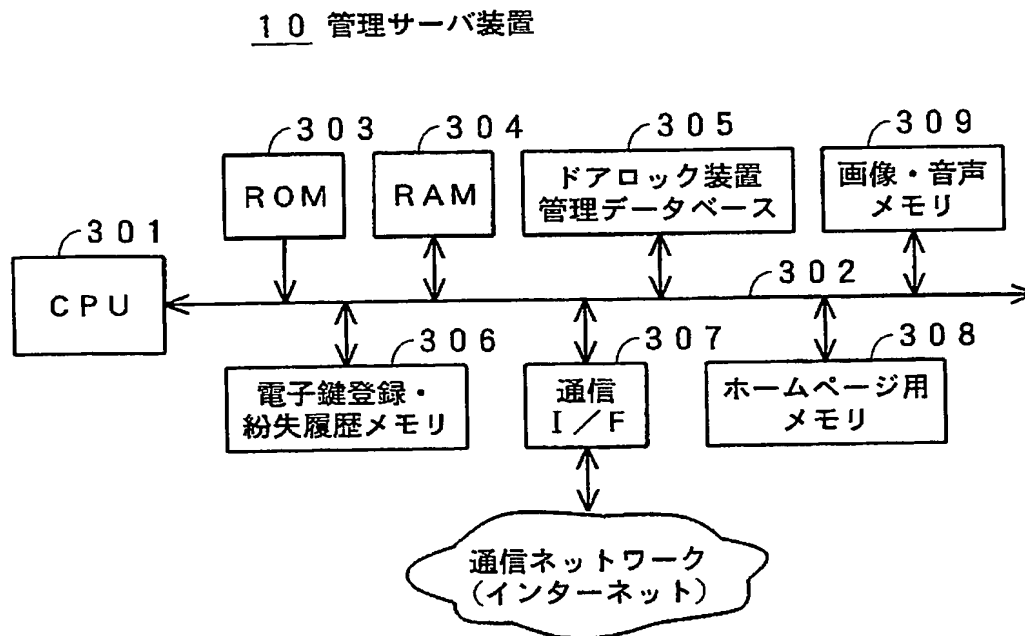
| セキュリティレベル | 父親 | 母親 | 子供 |
|-----------|----|----|----|
| D | ○ | ○ | ○ |
| D | ○ | ○ | × |
| D | ○ | × | ○ |
| D | ○ | × | × |
| C | × | ○ | ○ |
| C | × | ○ | × |
| B | × | × | ○ |
| A | × | × | × |

○：在宅
×：不在

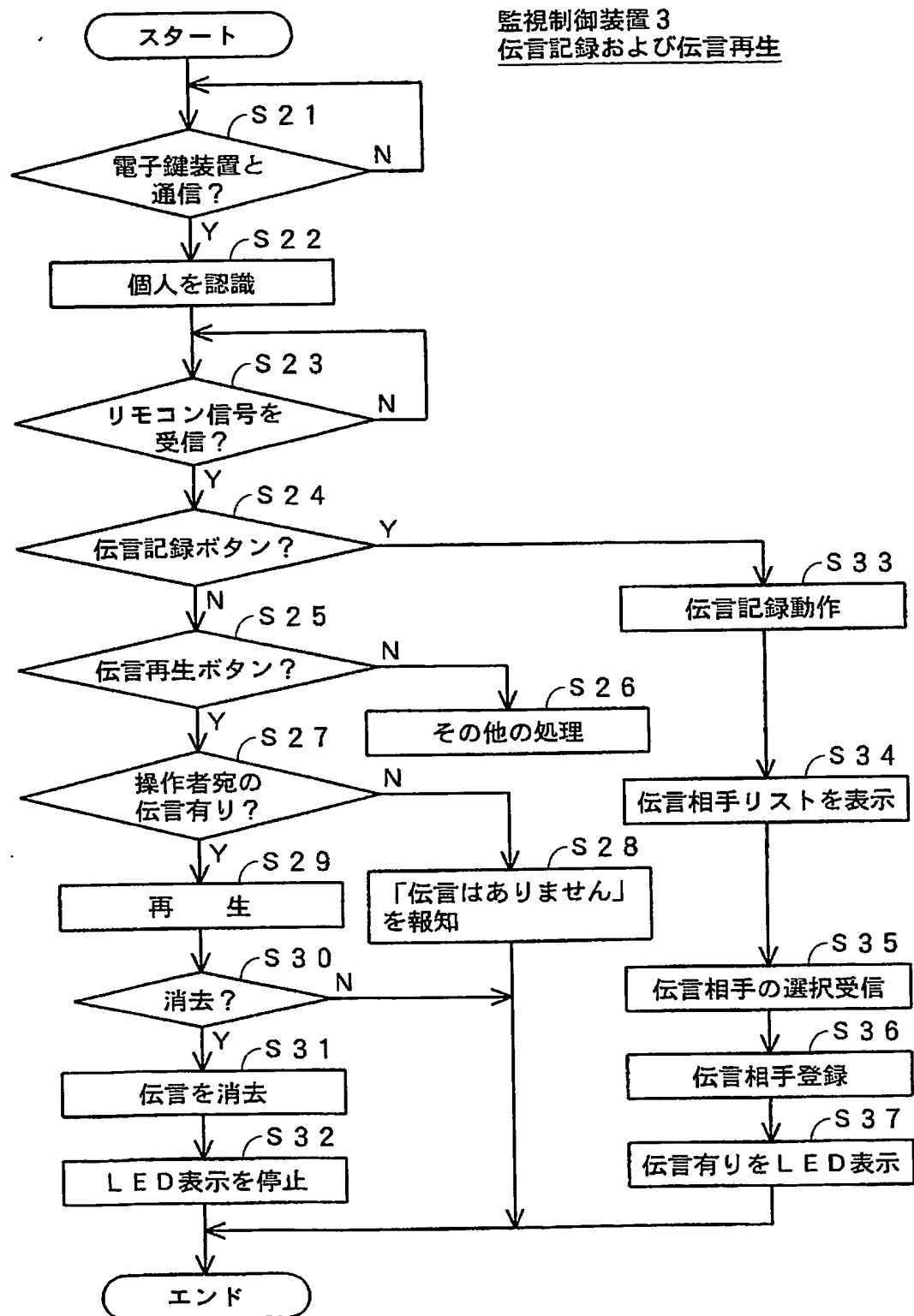
【図 16】

| セキュリティレベル | 窓・ドア監視 | 火災・ガス監視 | カメラ監視 |
|-----------|--------|---------|-------|
| A | ○ | ○ | ○ |
| B | ○ | ○ | × |
| C | × | ○ | × |
| D | × | × | × |

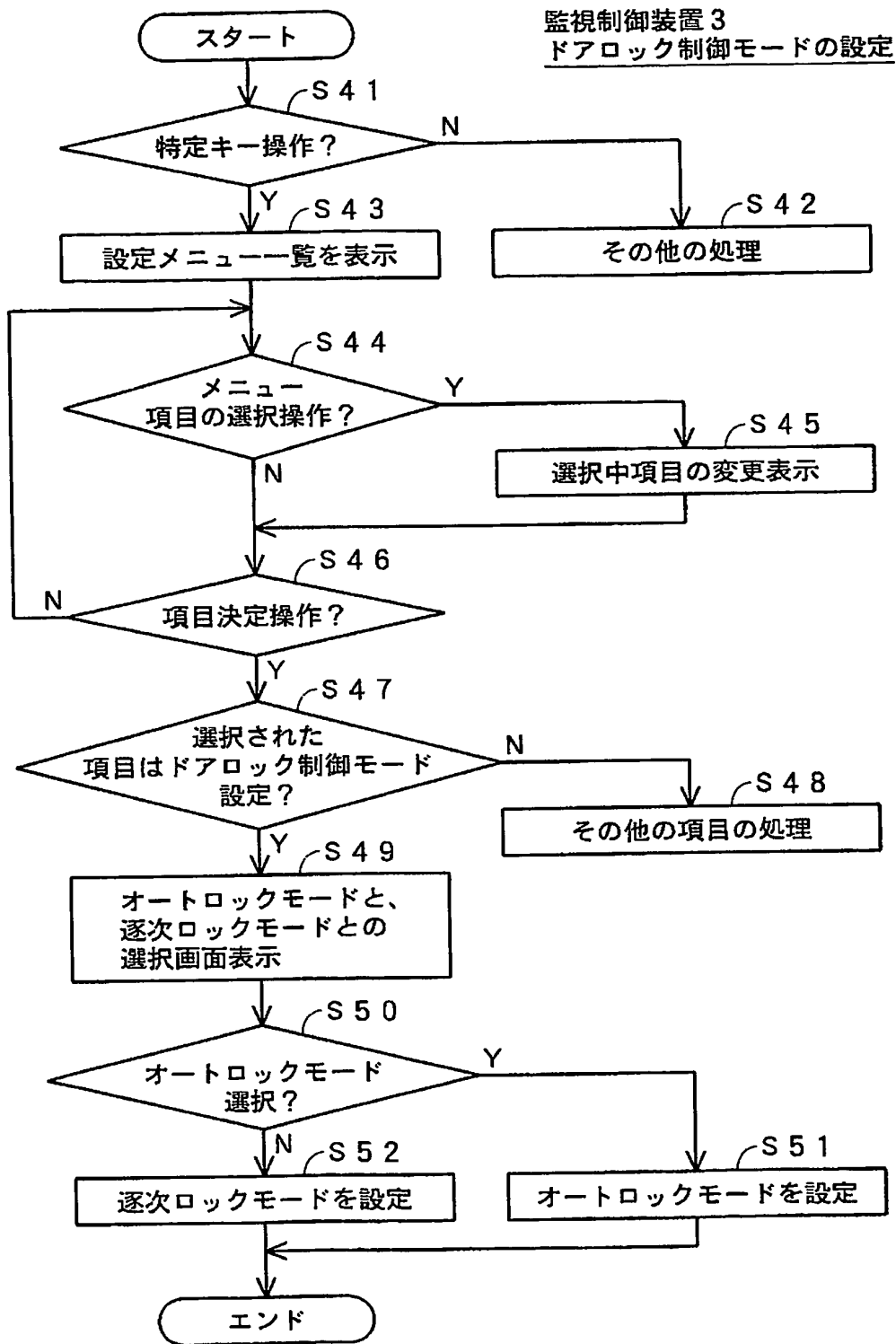
【図17】



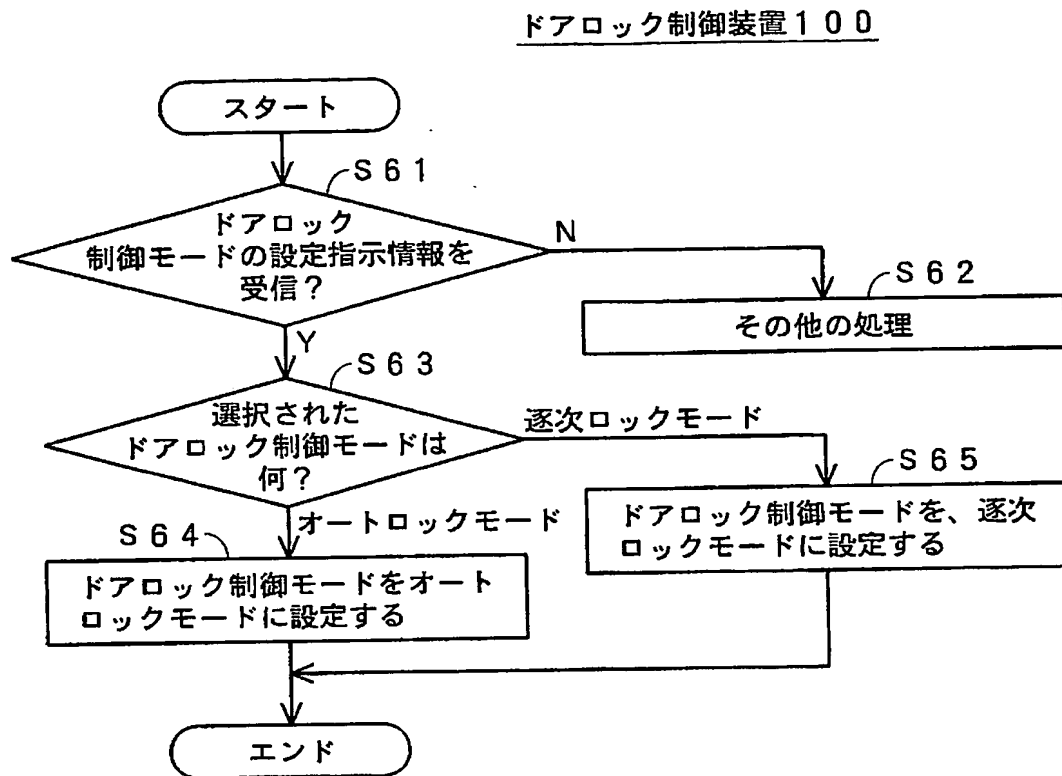
【図 18】



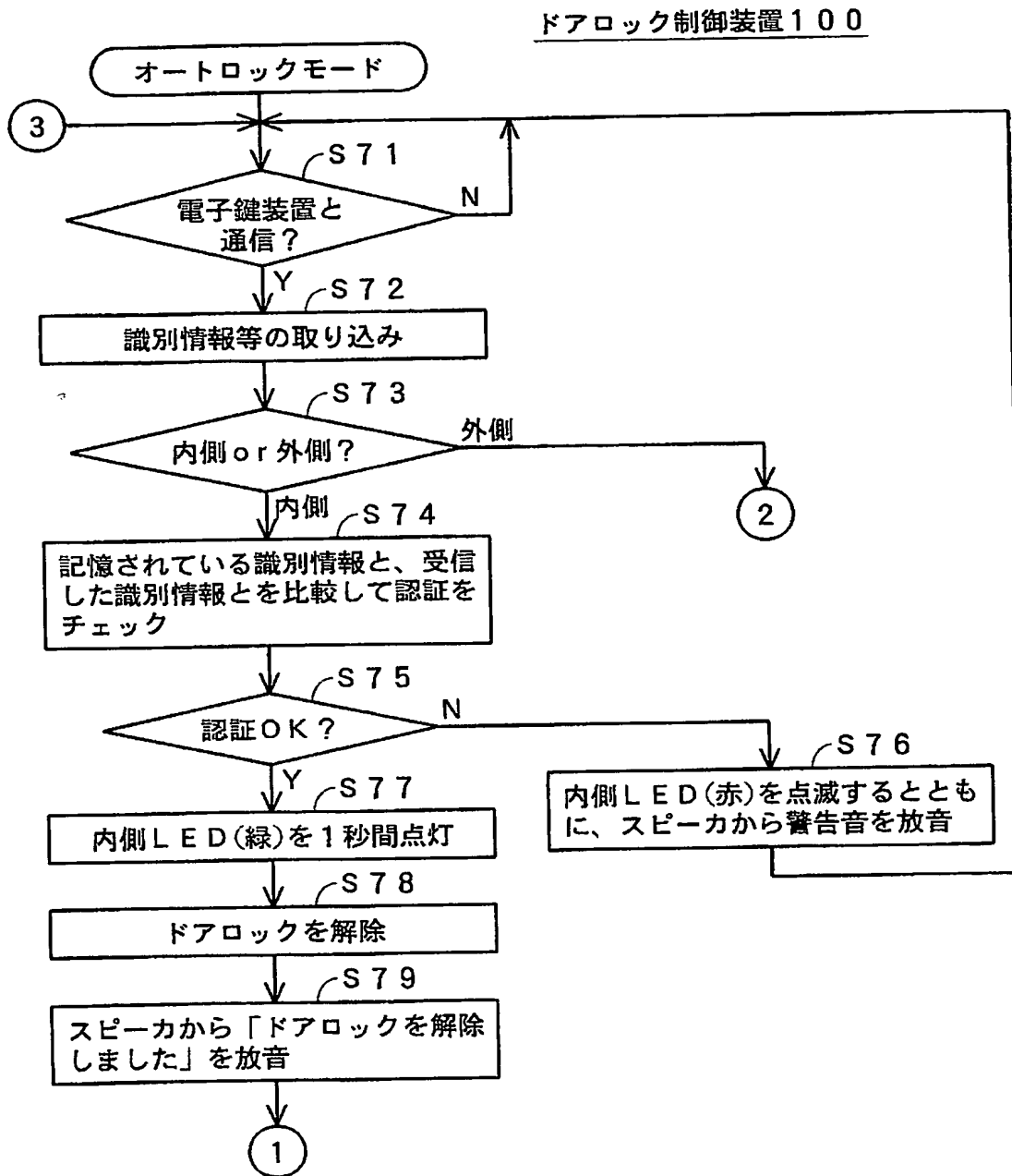
【図19】



【図20】

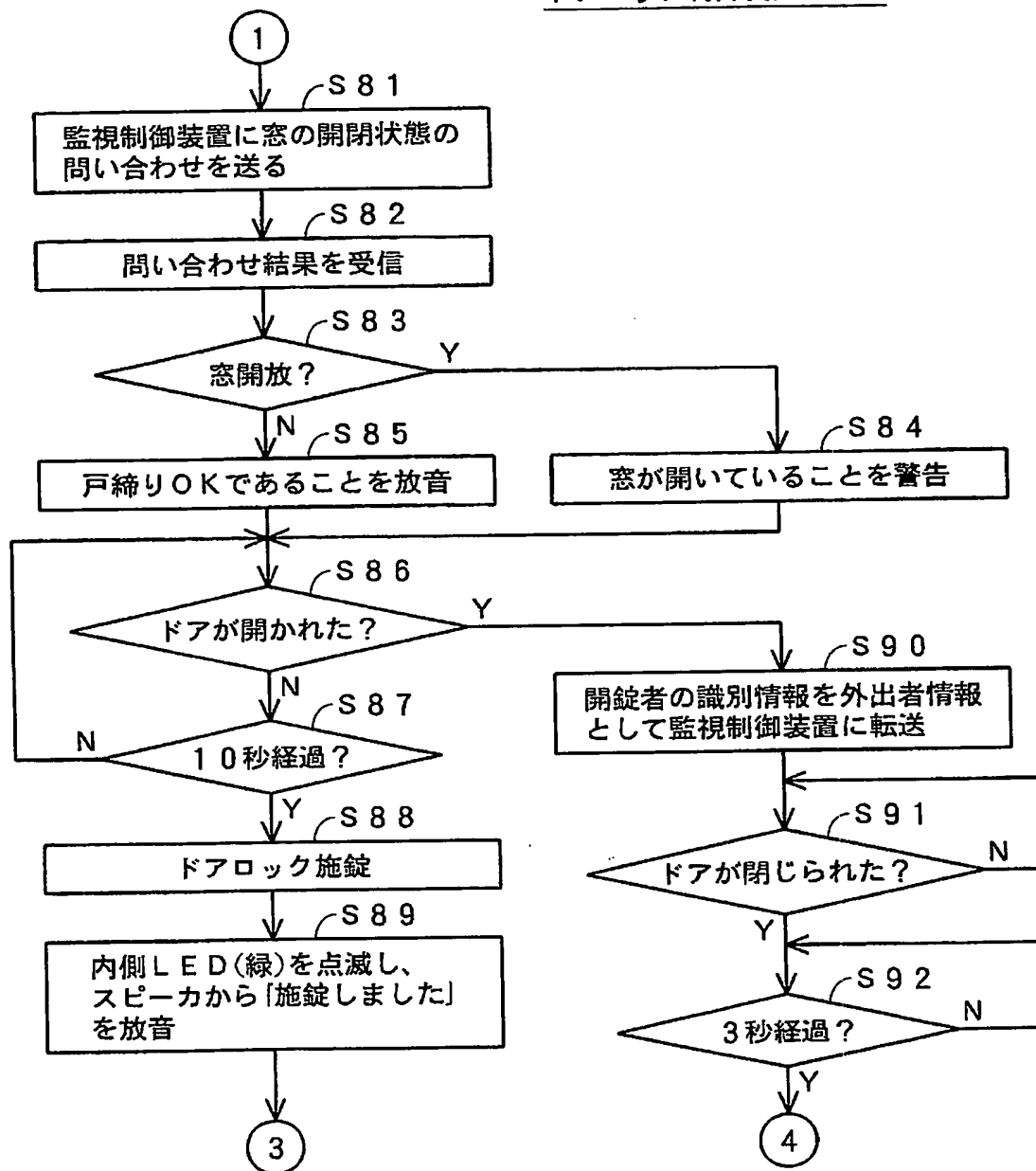


【図21】



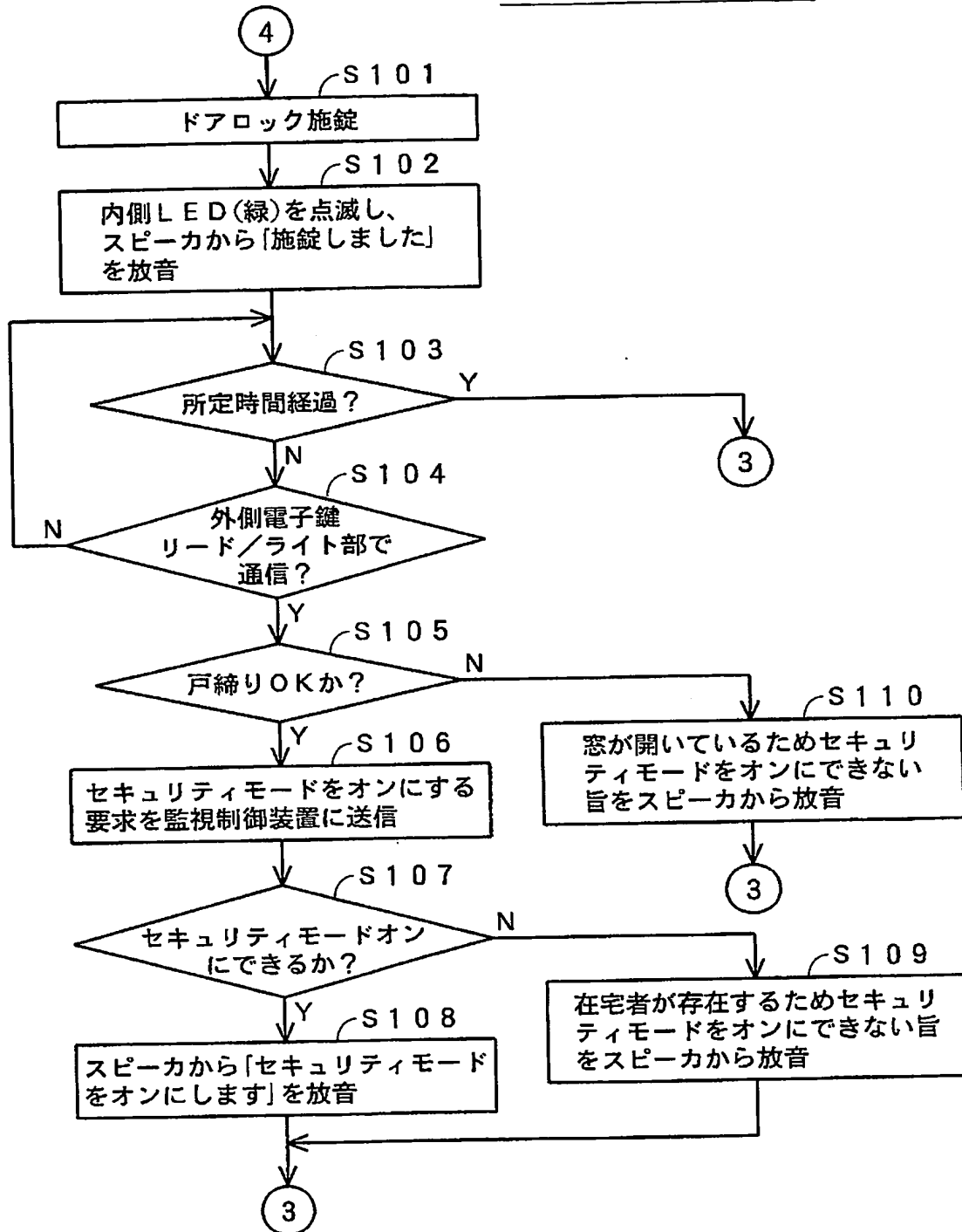
【図22】

ドアロック制御装置100



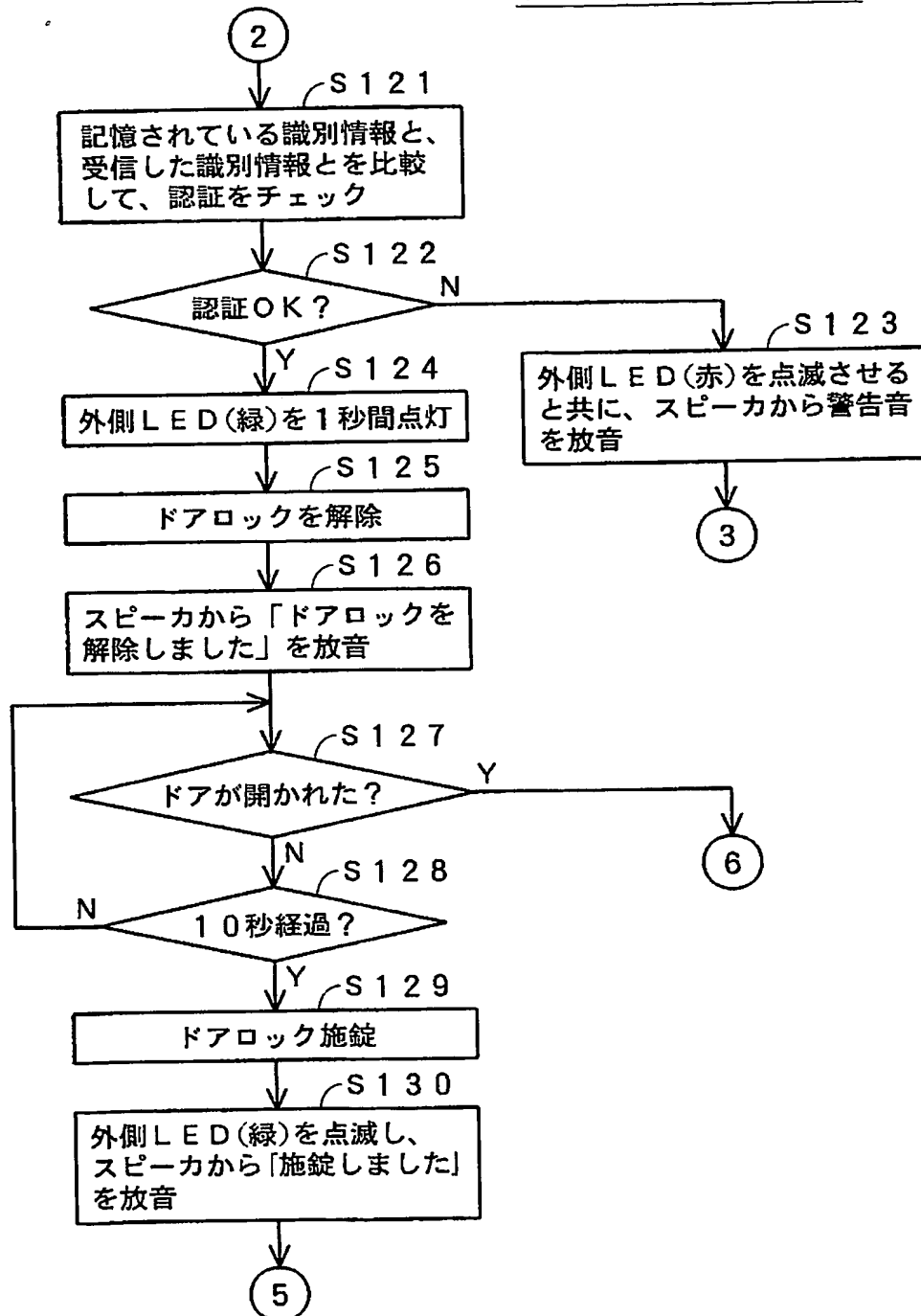
【図 23】

ドアロック制御装置 100



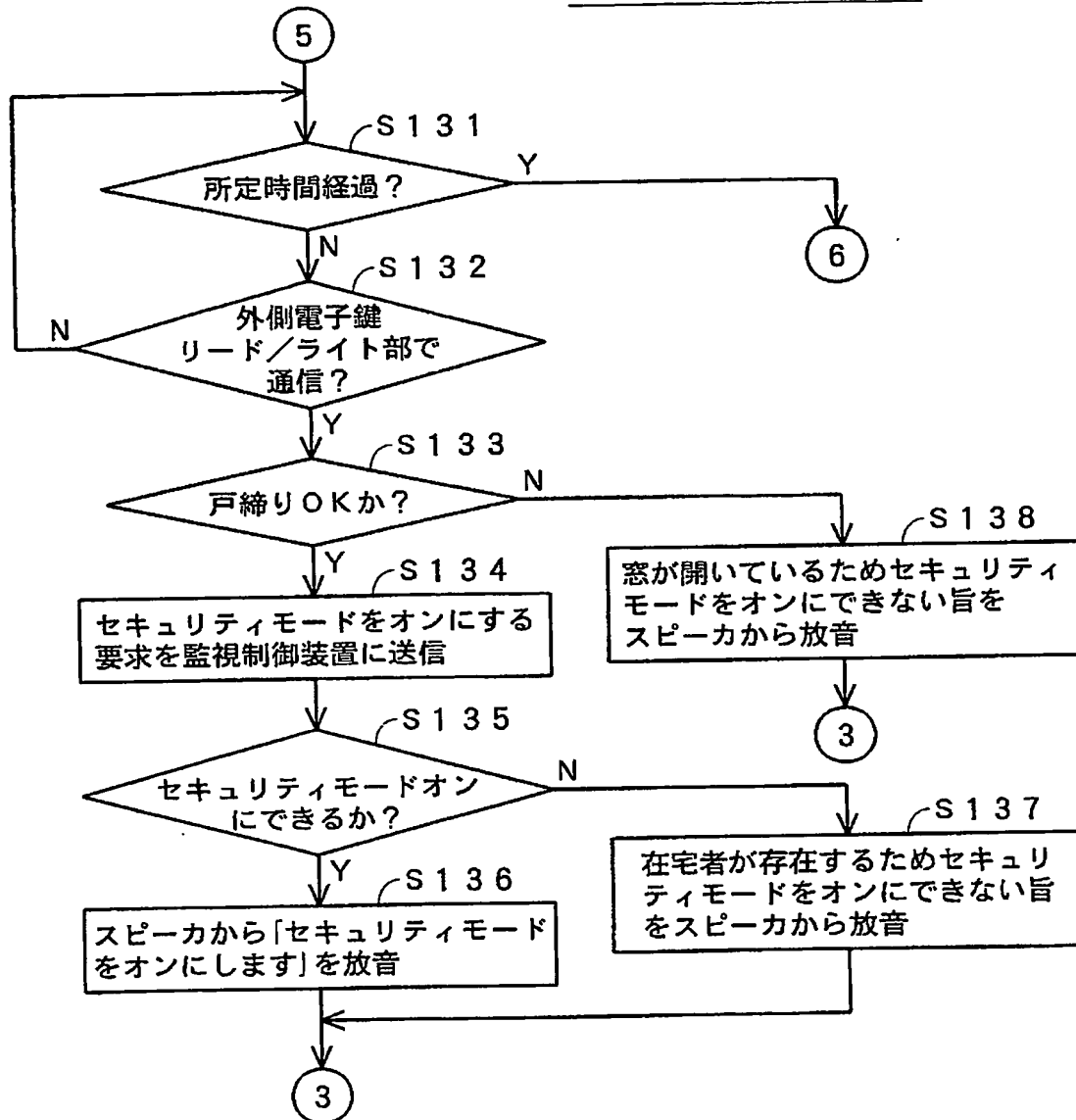
【図 24】

ドアロック制御装置 100



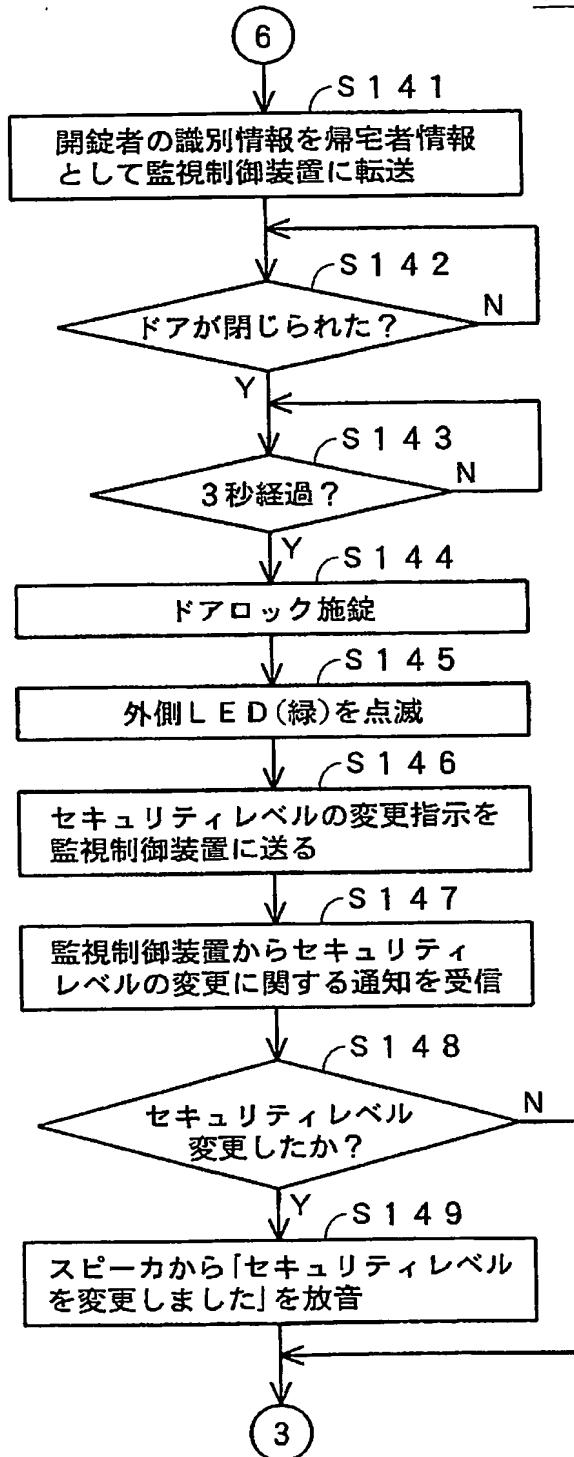
【図 25】

ドアロック制御装置 100

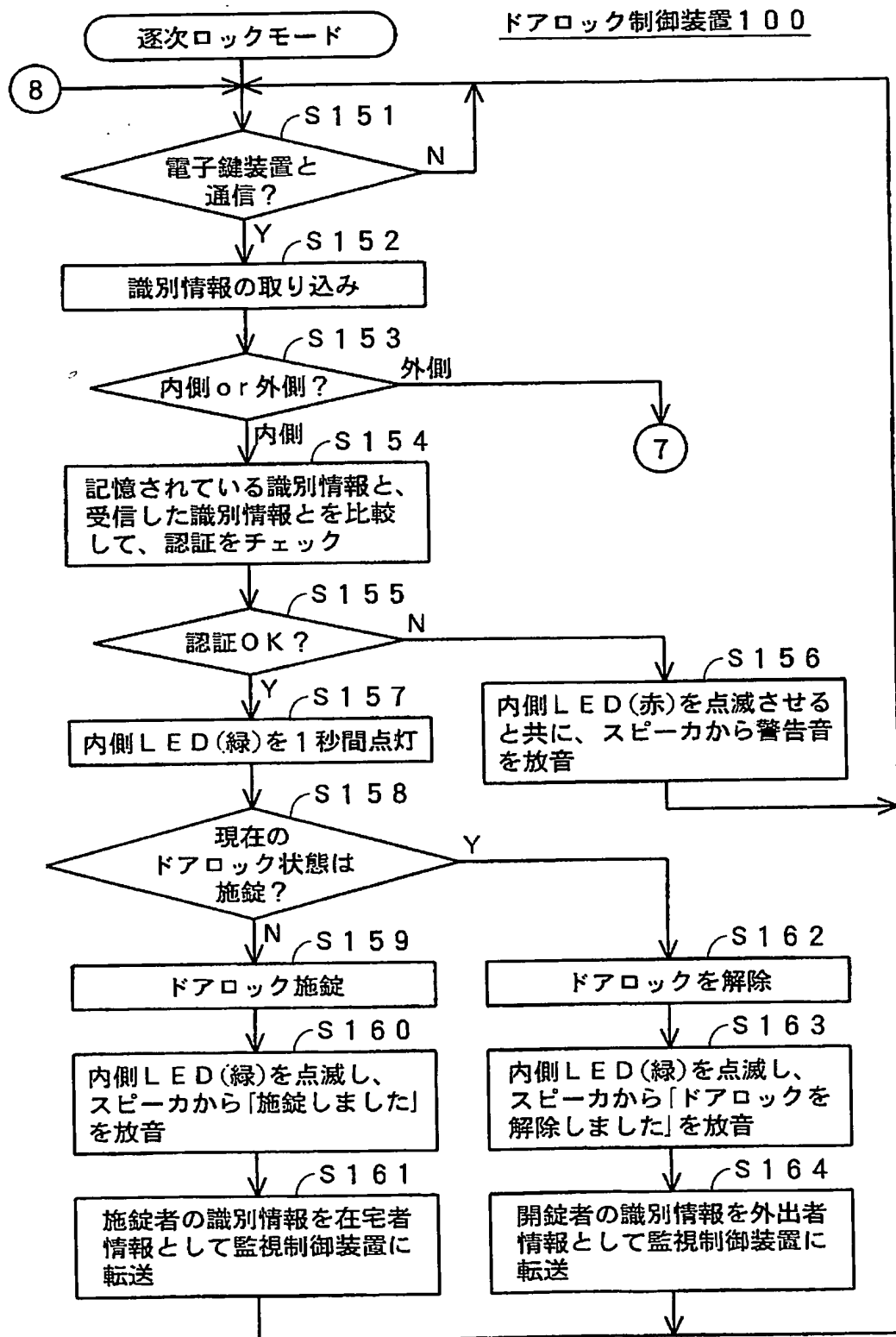


【図26】

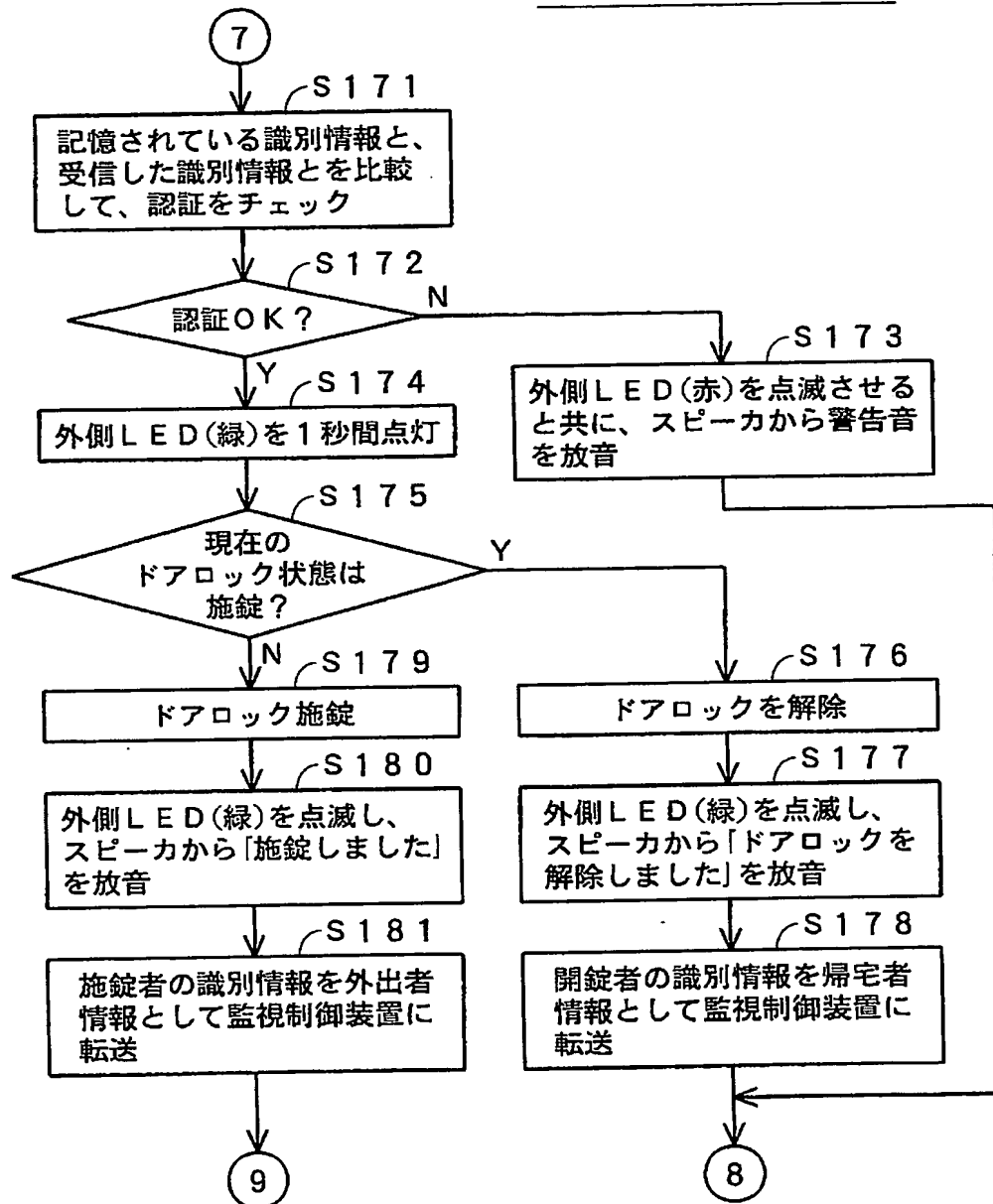
ドアロック制御装置1.0.0



【図27】

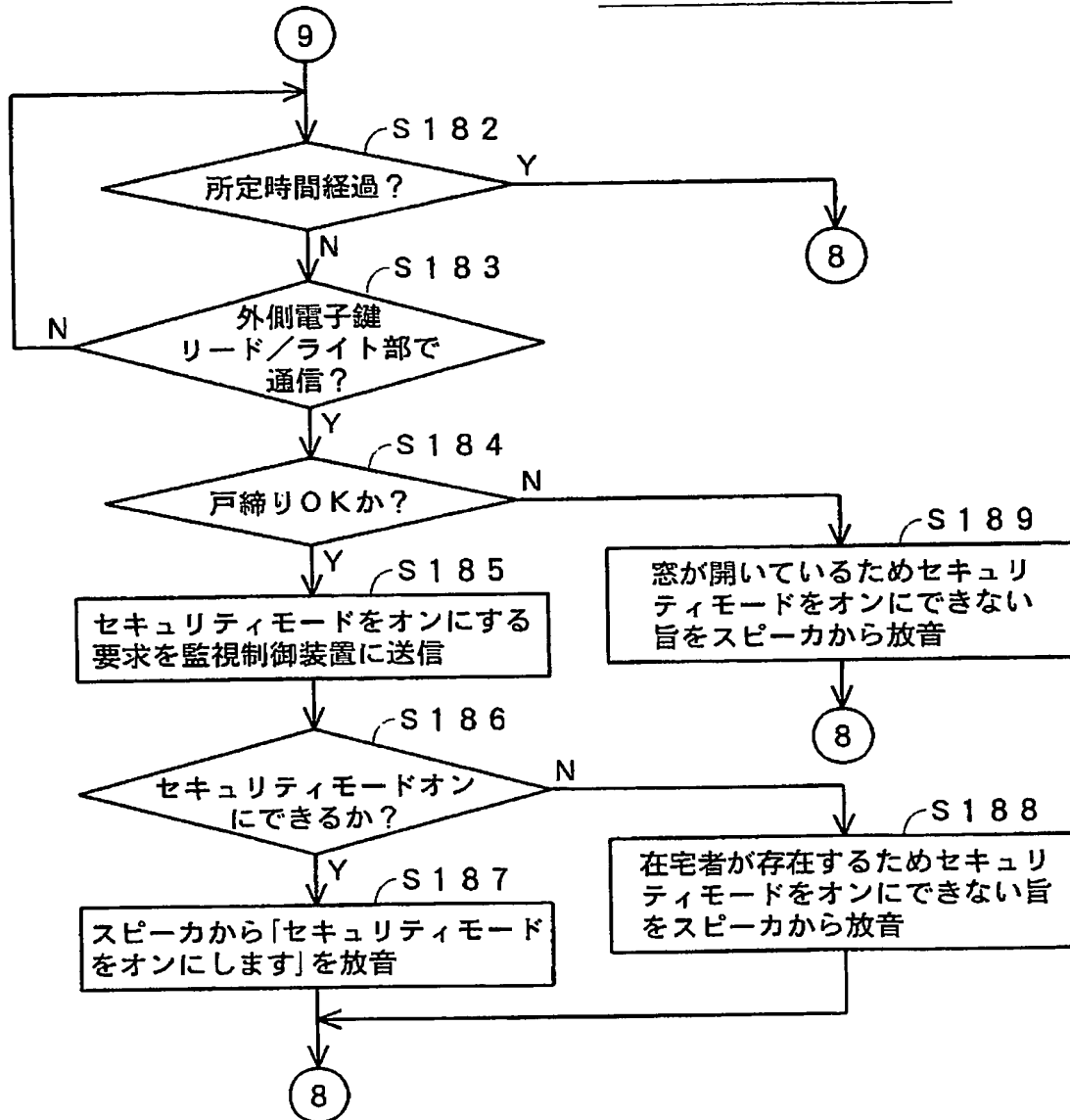


【図 28】

ドアロック制御装置 100

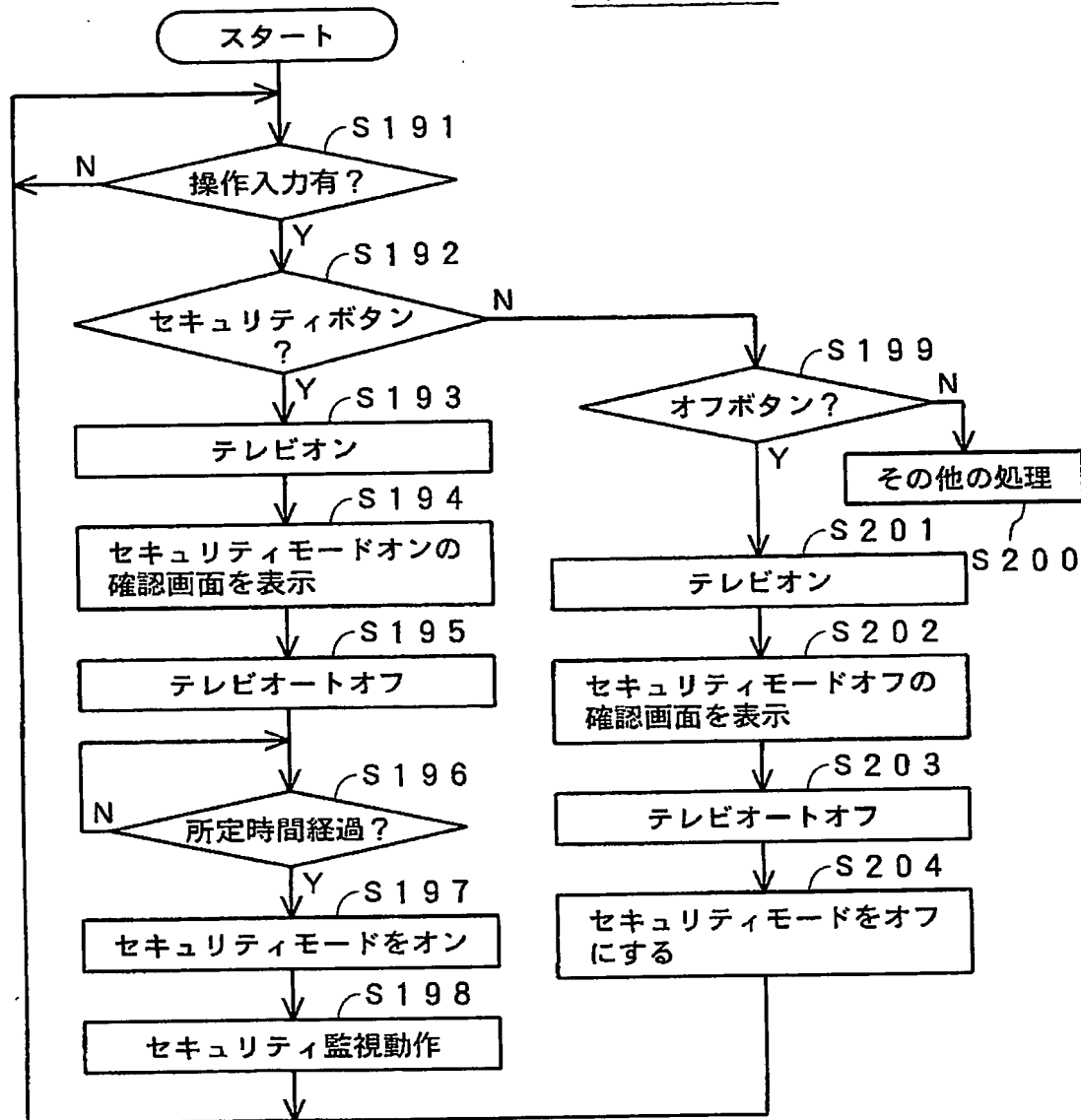
【図 29】

ドアロック制御装置 100

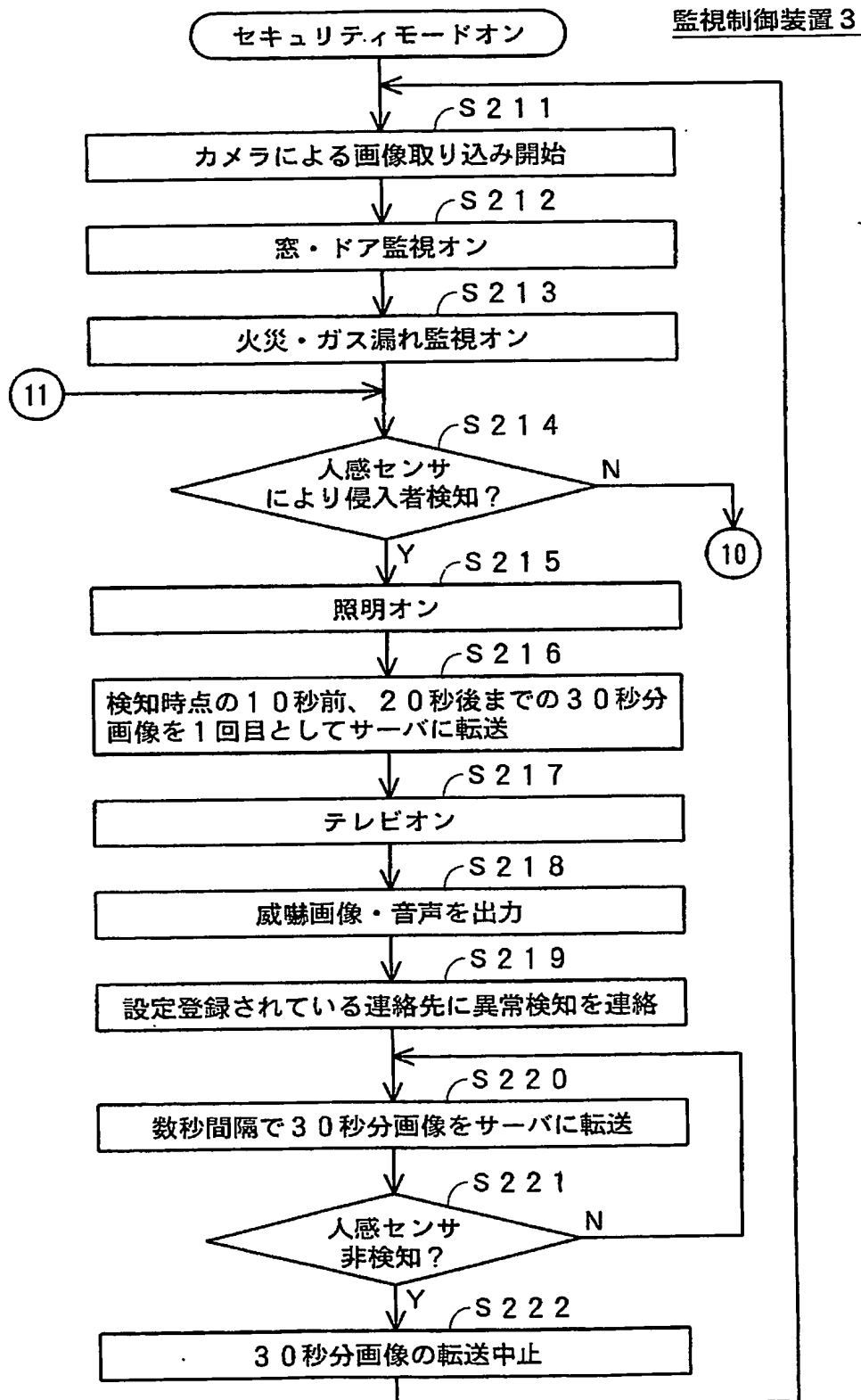


【図 30】

監視制御装置 3

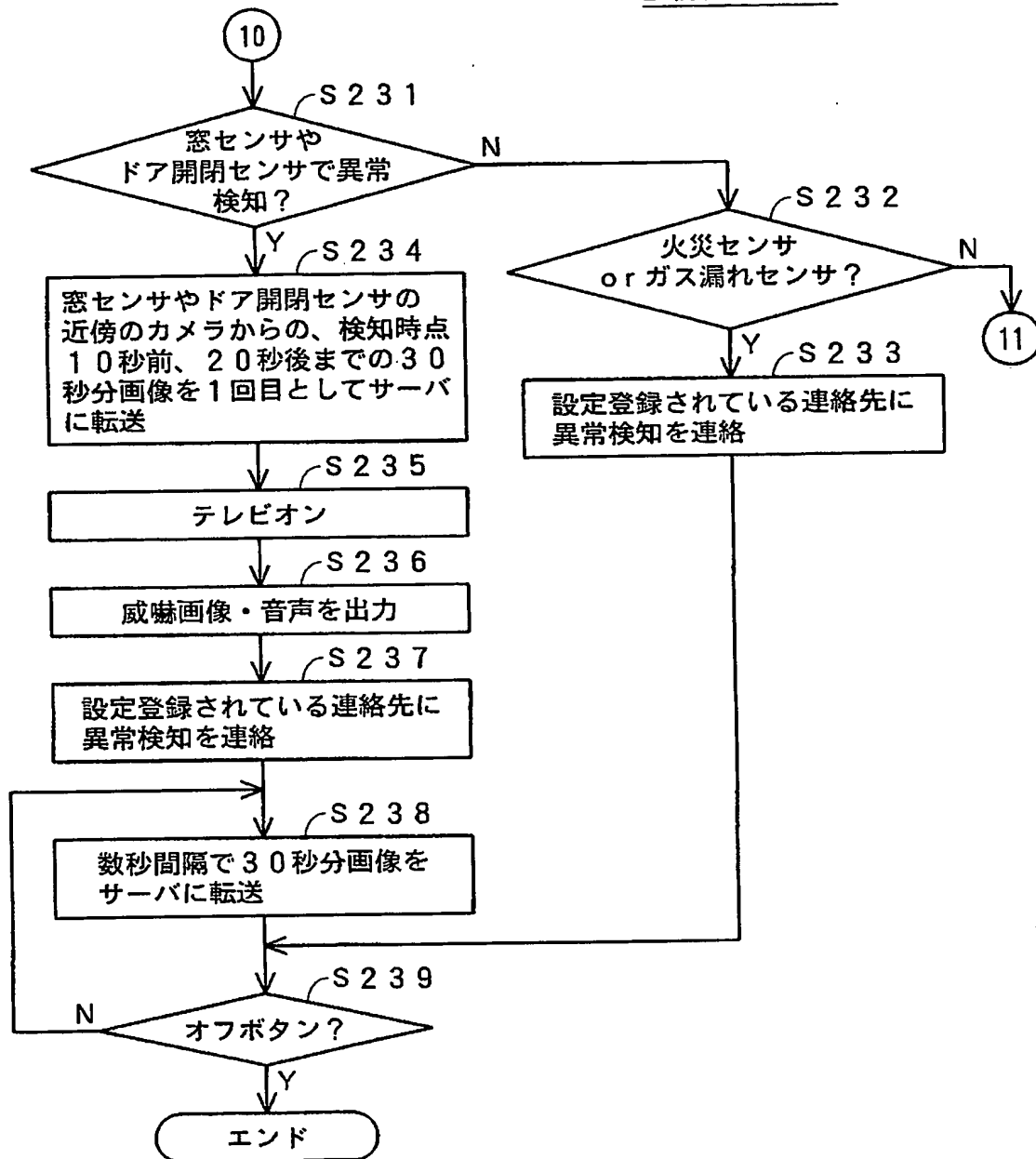


【図 31】

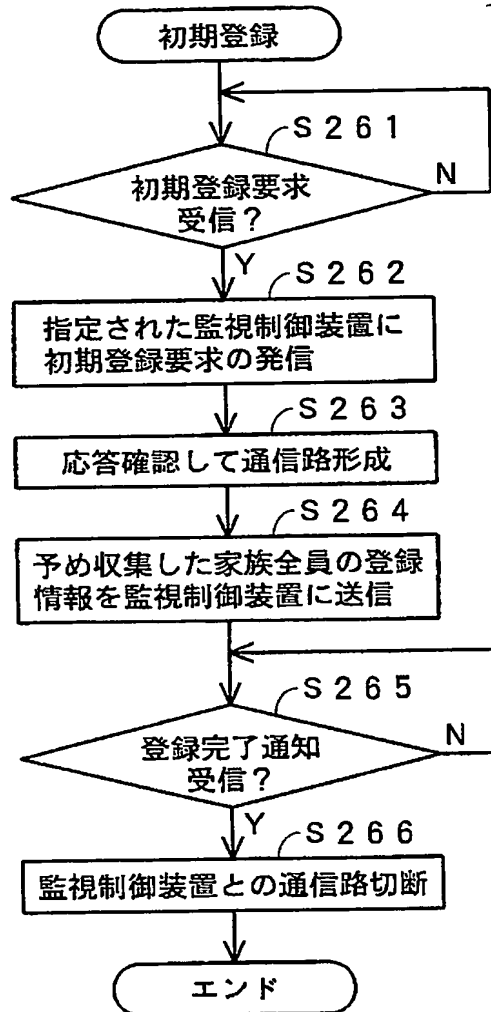


【図32】

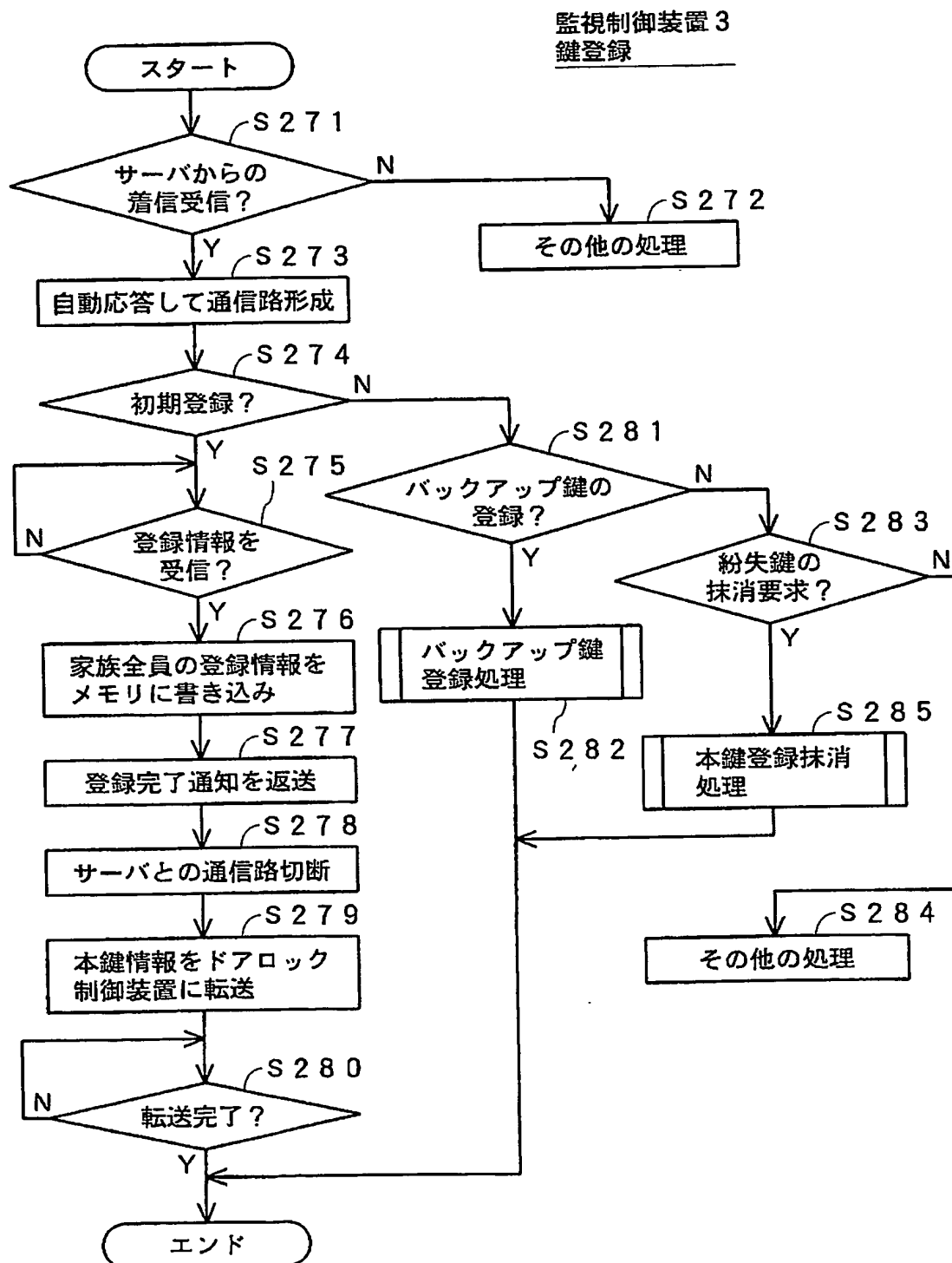
監視制御装置3



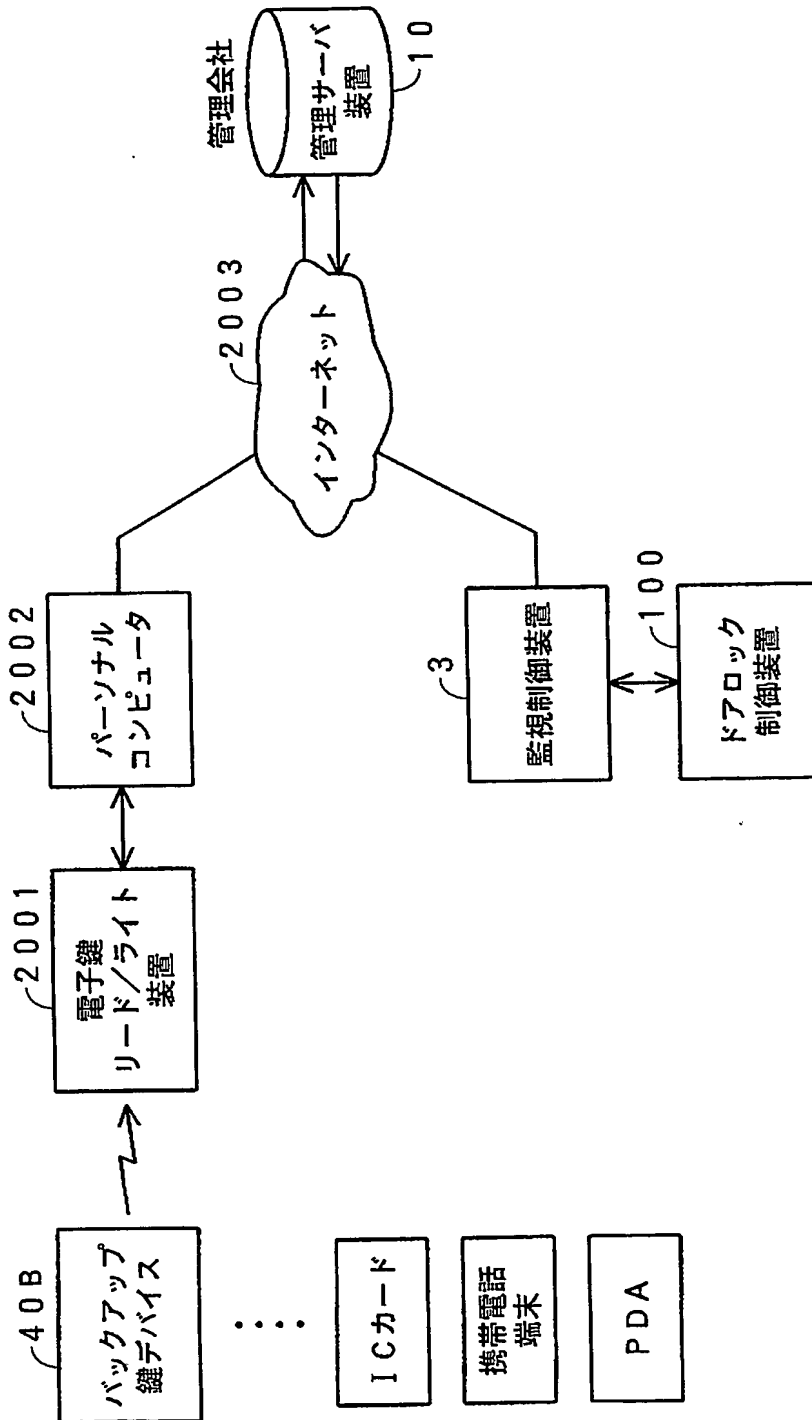
【図 34】

管理サーバ装置 10
初期登録

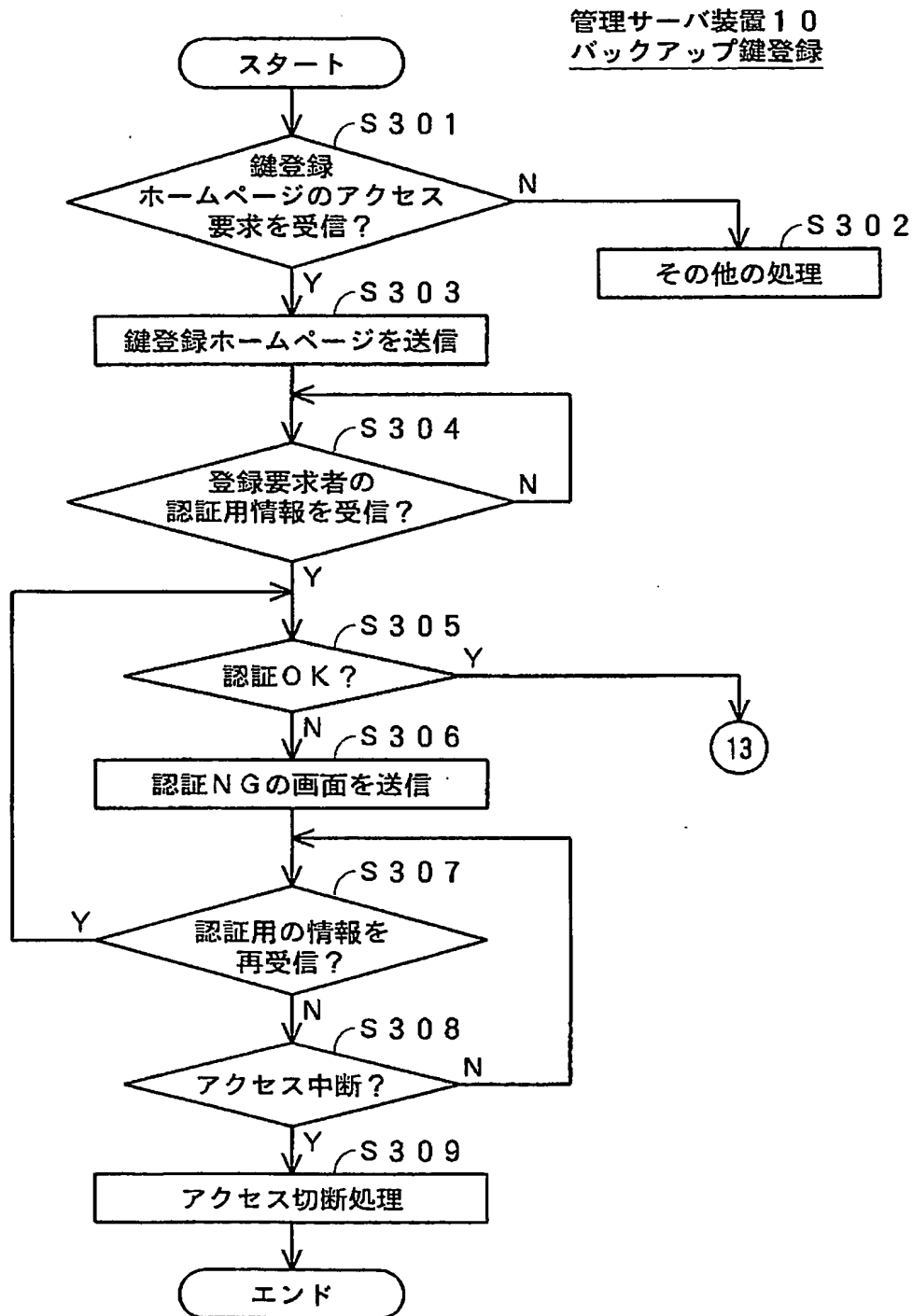
【図35】



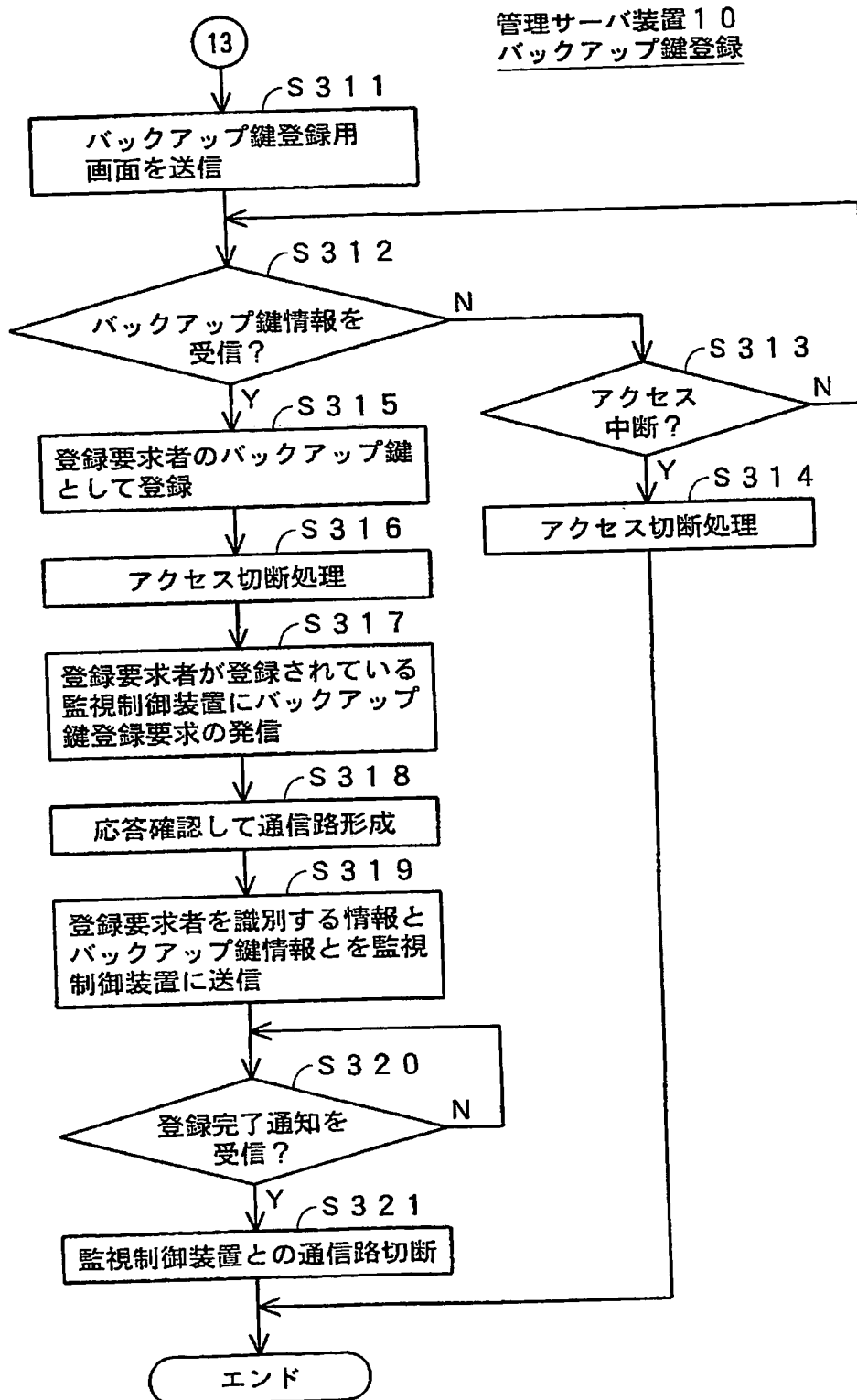
【図 36】



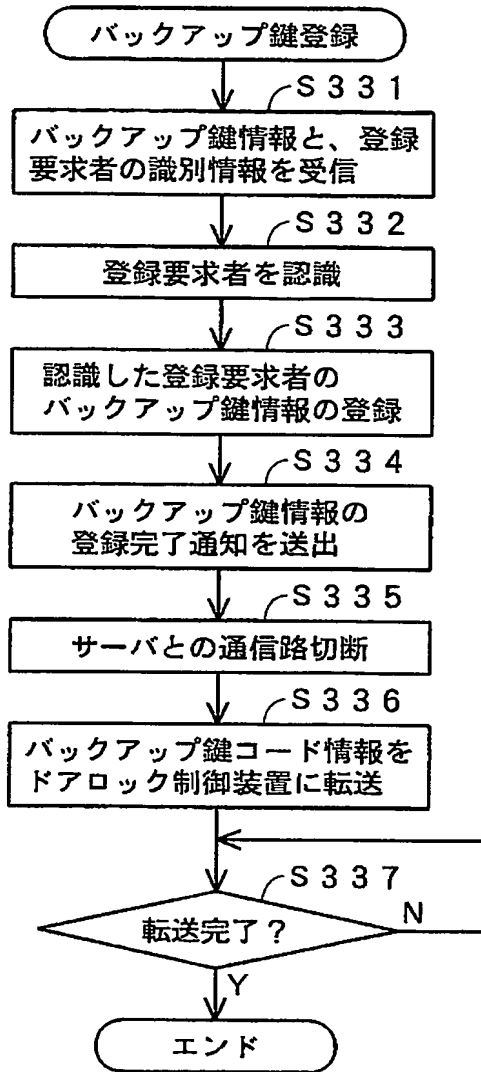
【図 37】



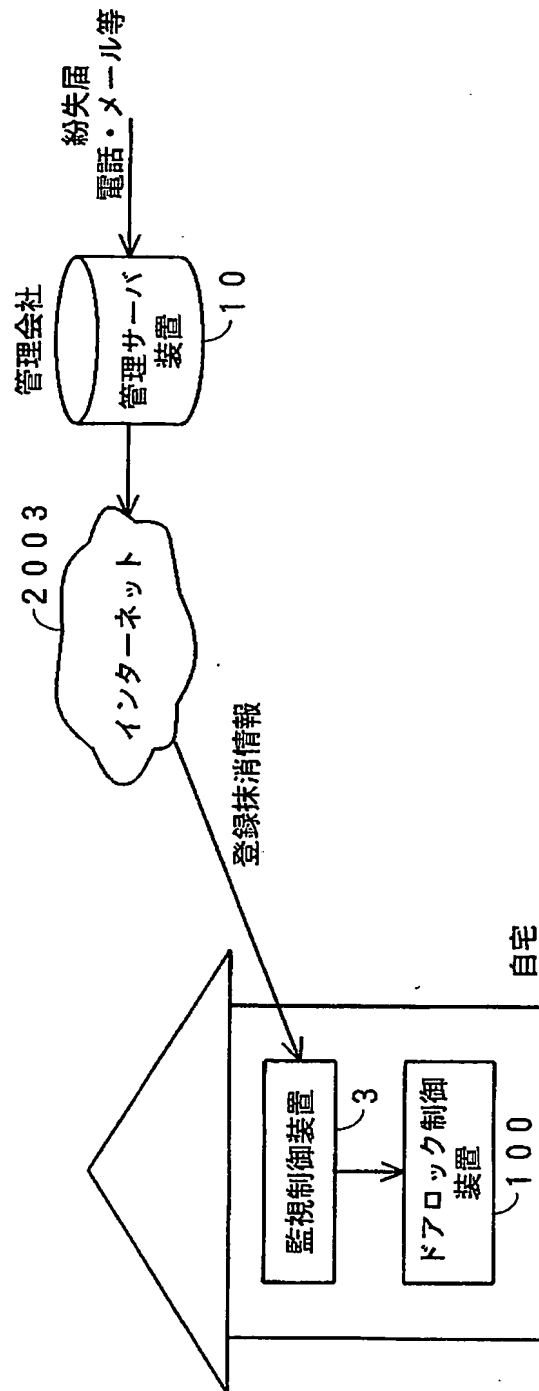
【図 38】



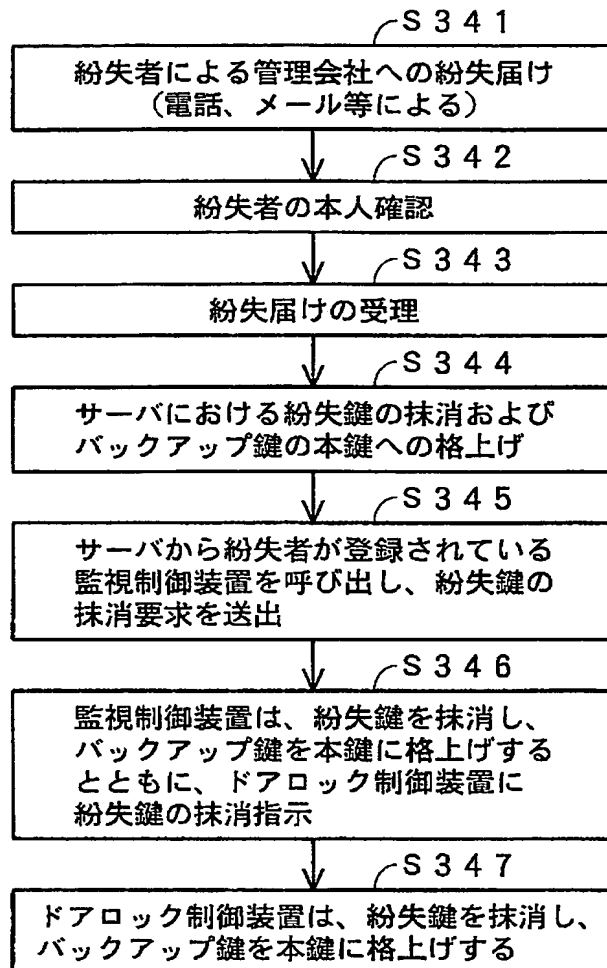
【図 39】

監視制御装置 3
バックアップ鍵登録

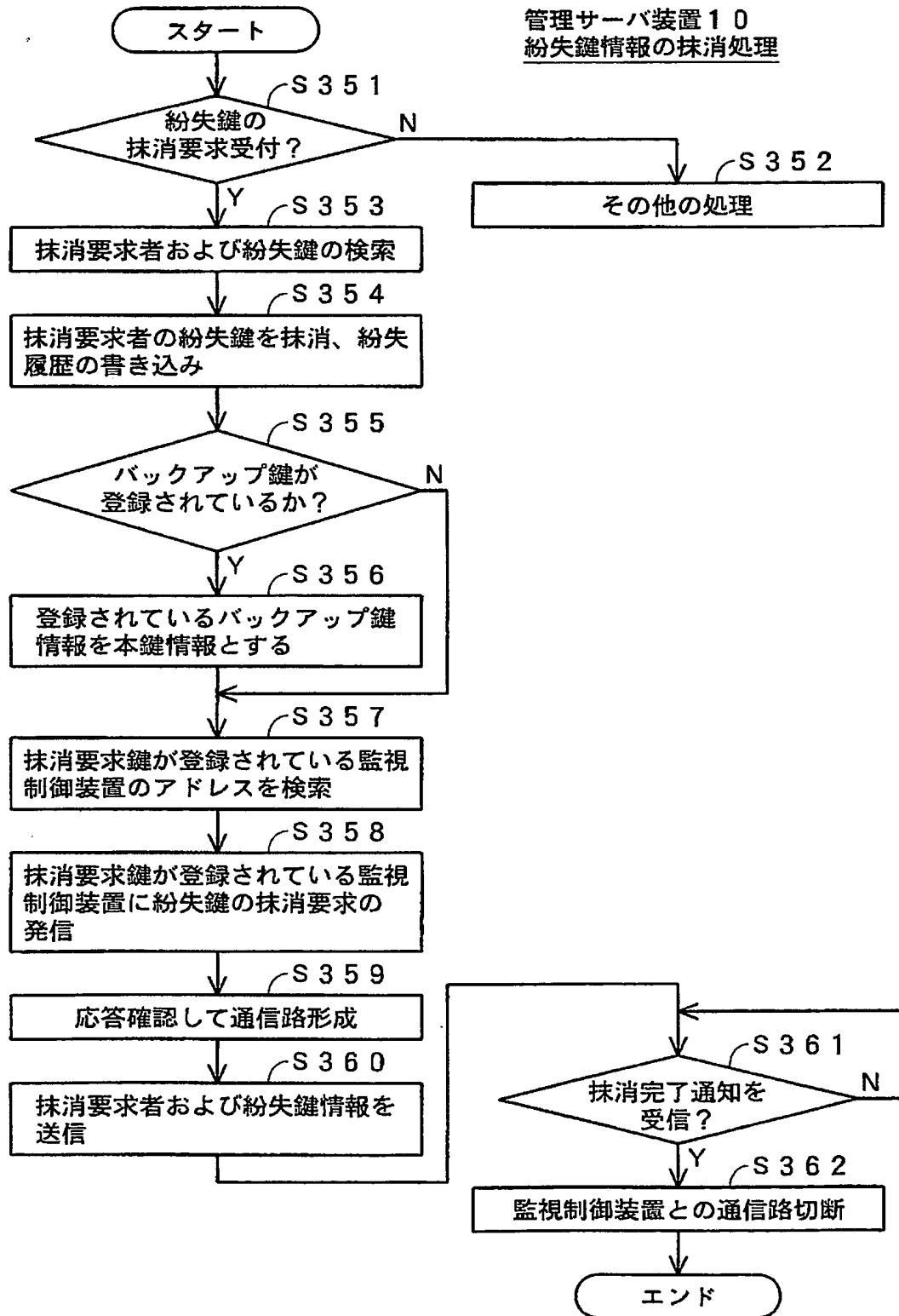
【図 40】



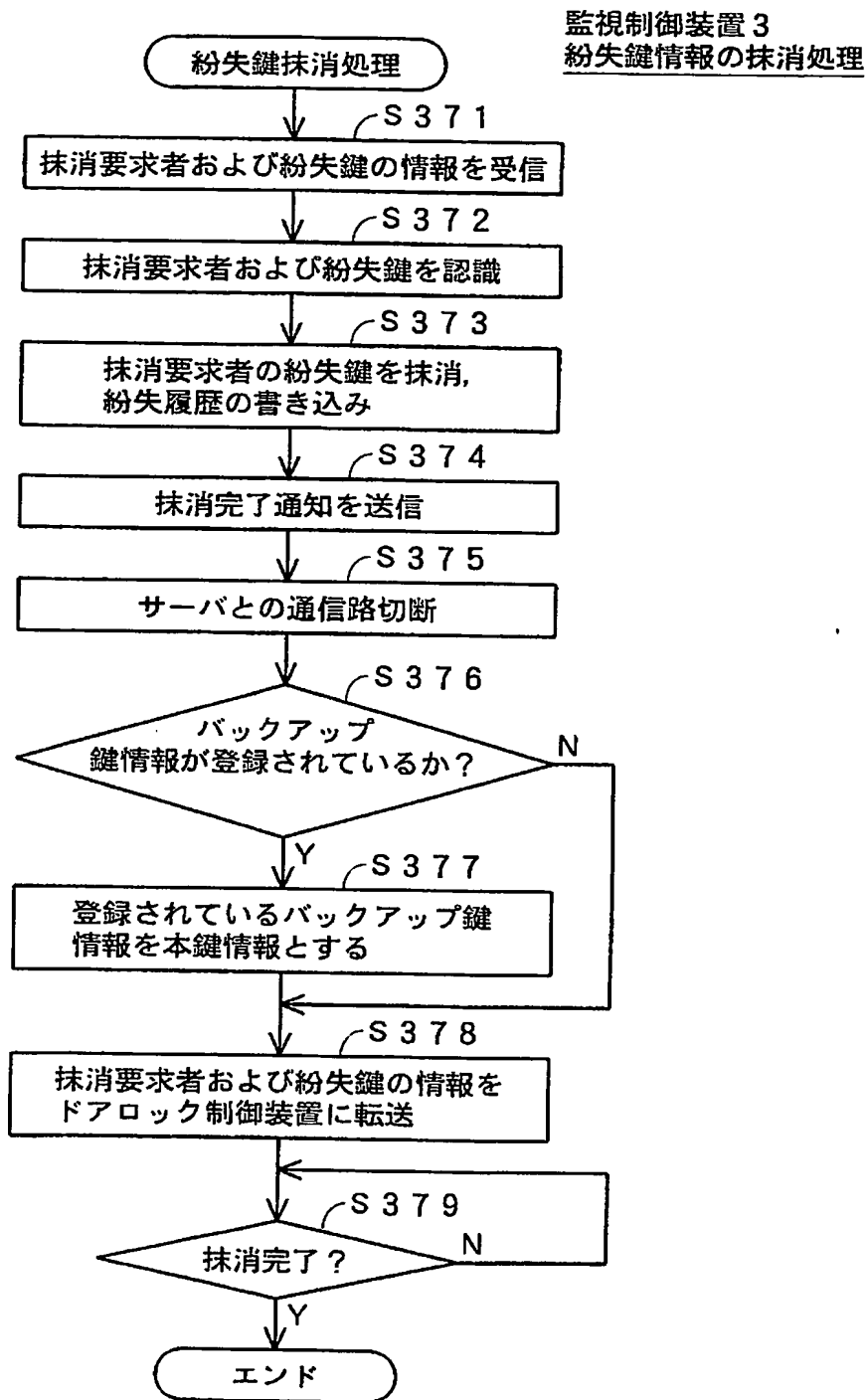
【図 4 1】

紛失鍵の抹消手順

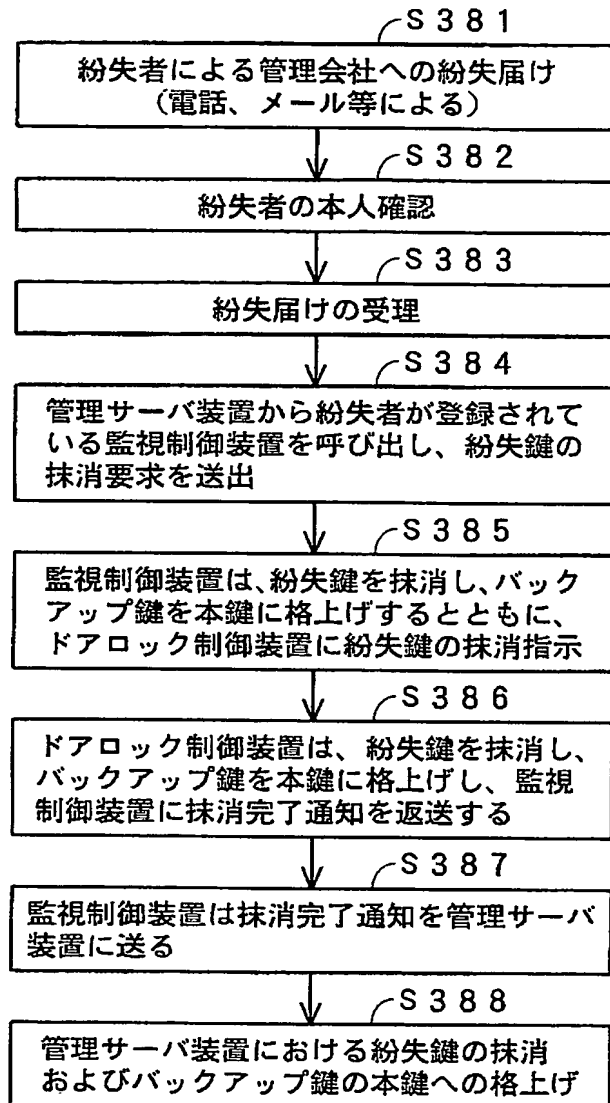
【図 4 2】



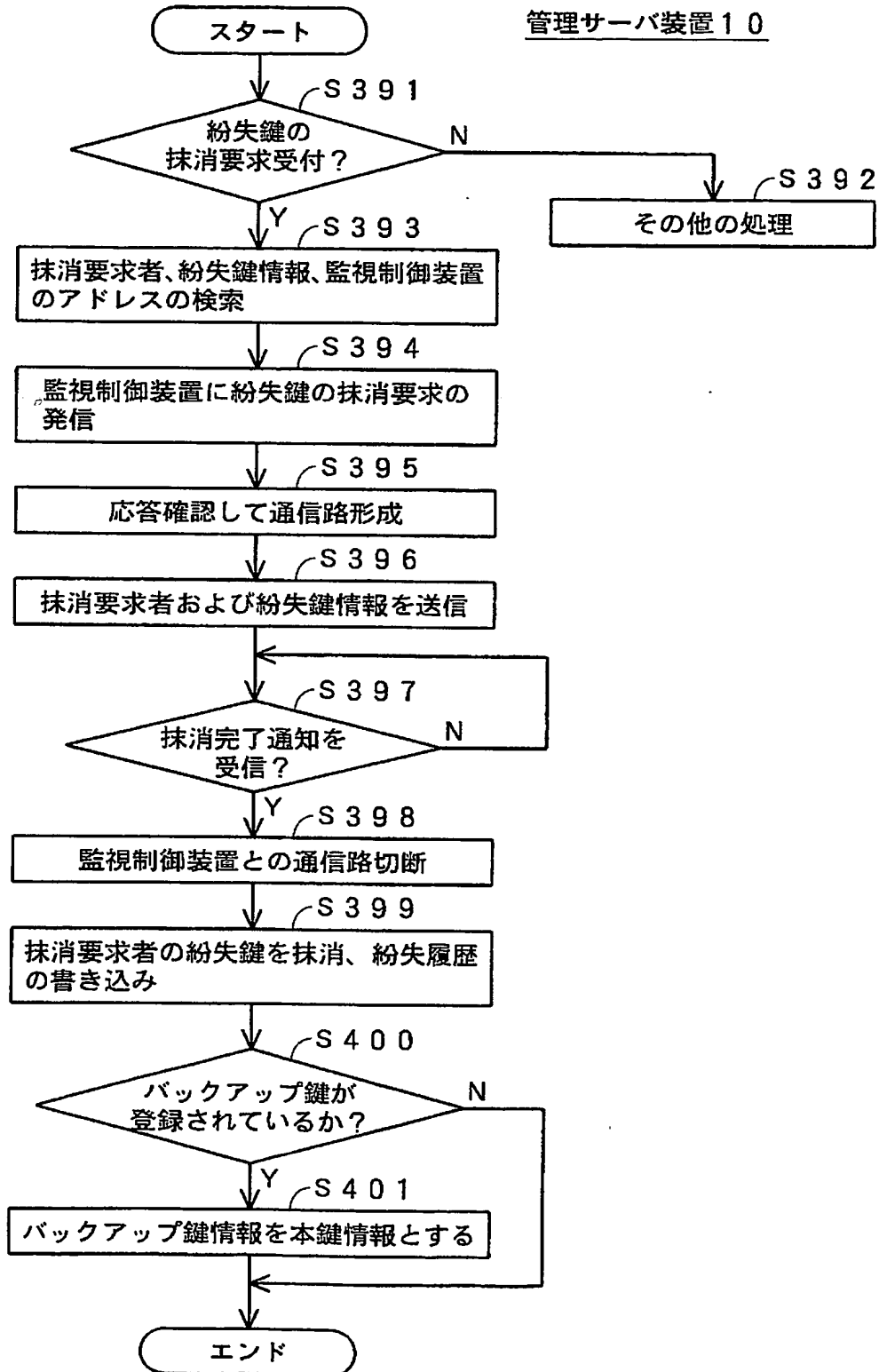
【図 43】



【図 44】

紛失鍵の抹消手順

【図 45】



【書類名】 要約書

【要約】

【課題】 紛失しても、容易に悪意の紛失鍵の拾得者に対抗することができる電子鍵装置を提供する。

【解決手段】 生体情報を取得する生体情報取得手段 41 と、生体情報が記憶されている生体情報記憶部 408 と、電子鍵情報が記憶されている電子鍵情報記憶部 405 と、電子鍵情報を外部に送信する機能を備える通信手段 42 と、生体情報取得手段 41 で取得された生体情報と、生体情報記憶部 408 に記憶されている生体情報とを比較する比較手段と、比較手段での比較結果に基づいて、電子鍵情報記憶部の電子鍵情報の通信手段 42 を通じた送出を制御する制御手段 401 とを備える。

【選択図】 図 5

特願 2 0 0 2 - 2 9 8 3 0 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.